IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	No. 2:21-cv-00137-RCY
	)	
vs.	)	
	)	JURY TRIAL DEMANDED
PALO ALTO NETWORKS, INC.,	)	
	)	
Defendant.	)	
	)	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Centripetal Networks, Inc. ("Centripetal") files this Amended Complaint for Patent Infringement and Demand for Jury Trial against Palo Alto Networks, Inc. ("Defendant" or "PAN") and allege as follows:

THE PARTIES

1. Plaintiff Centripetal is a corporation organized under the laws of the state of Delaware with its principal place of business at 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171.

2. PAN is a Delaware corporation doing business at 1410 Spring Hill Rd., Suite 300, McLean, VA 22102, and 12110 Sunset Hills Rd., Suite 200, Reston, Virginia 20190 with a corporate agent for service of legal process located at Corporation Service Company, 100 Shockoe Slip Fl 2, Richmond, VA, 23219-4100.

3. PAN regularly conducts and transacts business in Virginia, throughout the United States, and within the Eastern District of Virginia, and as set forth below, has committed and continues to commit, tortious acts of patent infringement within Virginia, including the Eastern District of Virginia. Further, PAN directly or indirectly uses, distributes,

markets, sells, and/or offers to sell throughout the United States, including in this judicial district, various network security products, including firewall products and services.

JURISDICTION AND VENUE

4. This action for patent infringement arises under the patent laws of the United States, 35 U.S.C. § 101 *et seq.* This court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

5. This Court has personal jurisdiction over PAN. PAN has conducted and continues to conducts business within the State of Virginia, and has engaged in continuous and systematic activities in the State of Virginia, including within this District. PAN maintains a regular and established place of business in this District through offices located at 1410 Spring Hill Rd., Suite 300, McLean, VA 22102, and 12110 Sunset Hills Rd., Suite 200, Reston, Virginia 20190. PAN, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, offers for sale, sells, and advertises (including by publishing an interactive web page in this District) their products and/or services in the Eastern District of Virginia, the State of Virginia, and the United States.

6. PAN, directly and through subsidiaries or intermediaries including distributors, retailers, and others, has purposefully and voluntarily placed one or more of their infringing products and/or services, as described below, into the stream of commerce with the expectation that they will be purchased and used by consumers in the Eastern District of Virginia. These infringing products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Virginia. PAN has committed acts of patent infringement within the State of Virginia and, more particularly, within the Eastern District of Virginia.

7. In addition, the Court has personal jurisdiction over PAN because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice. For example, PAN advertises active job listings in this District in the cities of Mclean, Reston, Richmond, and Centreville, including job listings for engineers, and makes, uses, offers for sale, and sells products or services that infringe the Asserted Patents in this District, as further described below.

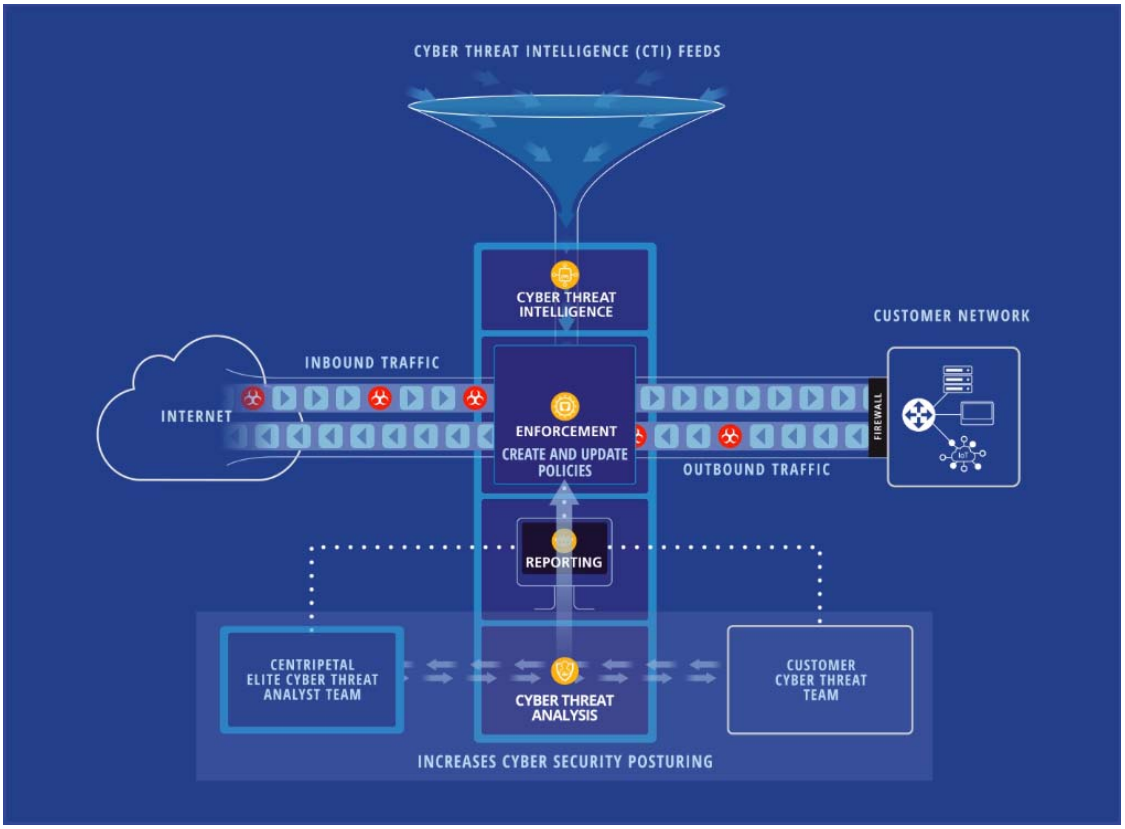
8. Venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 (b) and (c) and/or 1400(b). PAN has transacted business in this District, has a regular and established place of business in this District, and has infringed, induced infringement, and/or contributorily infringed in this District, and continues to do so. PAN maintains a regular and established place of business in this District described above. Centripetal is informed and believes that PAN employs a number of personnel in this District, including personnel involved in PAN's infringement by at least through the testing, demonstration, support, use, offer for sale, and sale of the Accused Products and services within Virginia.

CENTRIPETAL AND ITS INNOVATIONS

9. Centripetal was founded in 2009 with a core mission to lead the field in innovating security technology to protect computer networks from advanced threats. Indeed, Centripetal became the first in the field to develop and invent specialized core networking technologies to operationalize threat intelligence at a scale and speed that could address the challenge of the rapid growth in number and sophistication of cyber threats. Centripetal is the forerunner in developing cybersecurity technologies capable of fully operationalizing and automating threat intelligence at scale. These technologies protect organizations form advanced threats by extrapolating threat intelligence feeds and applying advanced packet

filtering at the network edge to prevent unwanted traffic from hitting an organization's network. Today, Centripetal maintains the largest threat intelligence partner ecosystem, providing community based solutions to defeat sophisticated cyberattacks.

10. Centripetal builds and sells software and appliances for network security using these patented technologies. Centripetal's CleanINTERNET® solutions utilize its patented Threat Intelligence Gateway, which allows organizations to eradicate threats based on threat intelligence enforcement and catch unknown threats.



Centripetal's patented technologies also provide insight into an organization's security posture and gain visibility into threats. Centripetal's Threat Intelligence Gateway includes the RuleGATE Gateway series, which are ultra-high performance threat intelligence gateways with real-time attack visualization and analytics. Ex. 13, CleanINTERNET® datasheet.

11. In recognition of its innovation and expertise, the U.S. Patent Office awarded Centripetal numerous patents that cover its key technological advances in the network security industry. Centripetal continues to apply for additional patents covering its innovations in the United States and around the world resulting directly from Centripetal's research and development efforts.

12. Centripetal has been recognized as an innovative technology company. For example, Centripetal was named the SINET 16 Innovator for 2017 at the SINET Showcase in Washington D.C. A leading research and advisory company, Gartner Research, recognized Centripetal as a Cool Vendor in Security for Technology and Service Providers in 2017. In both 2019 and 2020, Centripetal was ranked as one of the fastest growing technology companies in North America on Deloitte's 2020 Technology Fast 500.

CENTRIPETAL'S ASSERTED PATENTS

13. On January 21, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,542,028 (the "'028 Patent"), entitled "Rule-based Network-Threat Detection." The '028 patent application published on December 19, 2019 as US 2019/0387013. A true and correct copy of the '028 Patent is attached hereto as Exhibit 1.

14. The '028 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is by filtering network data packet transfers based on one or more rules corresponding to one or more network-threat indicators to facilitate the protection of computers and networks from network threats.

15. On August 25, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,757,126 (the "'126 Patent"), entitled "Rule-Based Network-

Threat Detection." The '126 patent application published on July 2, 2020 as US 2020/0213342. A true and correct copy of the '126 Patent is attached hereto as Exhibit 2.

16. The '126 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules corresponding to one or more network-threat indicators to facilitate the protection of computers and networks from network threats.

17. On January 7, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,530,903 (the "'903 Patent"), entitled "Correlating Packets in Communications Networks." The '903 patent application published on December 14, 2017 as US 2017/0359449. A true and correct copy of the '903 Patent is attached hereto as Exhibit 3.

18. The '903 Patent is generally directed towards computer networks, and more particularly, provides a system to improve the flow of data packets transferring between networks. One of the ways this is accomplished is generating log entries corresponding to the data packets and utilizing the log entries and the packets to correlate the packets transferred between the networks.

19. On May 19, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,659,573 (the "'573 Patent"), entitled "Correlating Packets in Communications Networks." The '573 patent application published on December 26, 2019 as US 2019/0394310. A true and correct copy of the '573 Patent is attached hereto as Exhibit 4.

20. The '573 Patent is generally directed towards computer networks, and more particularly, provides a system to improve the flow of data packets transferring between networks. One of the ways this is accomplished is generating log entries corresponding to the

data packets and utilizing the log entries and the packets to correlate the packets transferred between the networks.

21. On February 18, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,567,437 (the "'437 Patent"), entitled "Methods and Systems for Protecting a Secured Network." The '437 patent application published on July 25, 2019 as US 2019/0230128. A true and correct copy of the '437 Patent is attached hereto as Exhibit 5.

22. The '437 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from attacks. One of the ways this is accomplished is filtering network data packet transfers based on dynamic security policies to facilitate the protection of computers and networks from network threats.

23. On September 22, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,785,266 (the "'266 Patent"), entitled "Methods and Systems for Protecting a Secured Network." The '266 patent application published on April 30, 2020 as US 2020/0137121. A true and correct copy of the '266 Patent is attached hereto as Exhibit 6.

24. The '266 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from attacks. One of the ways this is accomplished is filtering network data packet transfers based on dynamic security policies to facilitate the protection of computers and networks from network threats.

25. On February 18, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,567,343 (the "'343 Patent"), entitled "Filtering Network Data Transfers." The '343 patent application published on May 3, 2018 as US 2018/0123955. A true and correct copy of the '343 Patent is attached hereto as Exhibit 7.

26. The '343 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules to facilitate the protection of computers and networks from network threats.

27. On August 4, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,735,380 (the "'380 Patent"), entitled "Filtering Network Data Transfers." The '380 patent application published on June 11, 2020 as US 2020/0186498. A true and correct copy of the '380 Patent is attached hereto as Exhibit 8.

28. The '380 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules to facilitate the protection of computers and networks from network threats.

29. On December 10, 2019, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,503,899 (the "'899 Patent"), entitled "Cyberanalysis Workflow Acceleration." The '899 patent application published on January 10, 2019 as US 2019/0012456. A true and correct copy of the '899 Patent is attached hereto as Exhibit 9.

30. The '899 Patent is generally directed towards computer networks, and more particularly, provides a system to improve analysis related to computer network security. One of the ways this is accomplished is using a communications monitoring device that may receive threat detection rules configured to cause the monitoring device to identify communications events that correspond to the threat detection rules.

31. On August 18, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,749,906 (the "'906 Patent"), entitled "Methods and Systems

for Protecting a Secured Network." The '906 patent application published on October 10, 2019 as US 2019/0312911. A true and correct copy of the '906 Patent is attached hereto as Exhibit 10.

32. The '906 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is by using a dynamic security policy with packet filtering rules automatically created by a security policy management server using malicious traffic information received from a malicious host tracker service.

33. On October 2, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,091,246 (the "'246 Patent"), entitled "Methods and Systems for Protecting a Secured Network." The '246 patent application published on December 14, 2017 as US 2017/0359382. A true and correct copy of the '246 Patent is attached hereto as Exhibit 11.

34. The '246 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is by using a dynamic security policy with packet filtering rules automatically created by a security policy management server and that use network addresses.

35. On February 18, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,567,413 (the "'413 Patent"), entitled "Rule-Based Network-Threat Detection." The '343 patent application published on August 1, 2019 as US 2019/0238577. A true and correct copy of the '413 Patent is attached hereto as Exhibit 12.

36. The '413 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the

ways this is accomplished is by filtering network data packet transfers based on one or more rules corresponding to one or more network-threat indicators from network threat intelligence providers to facilitate the protection of computers and networks from network threats.

37. On February 23, 2021, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,931,797 (the "'797 Patent"), entitled "Correlating Packets in Communications Networks." The '797 patent application published on August 6, 2020 as US 2020/0252486A1. A true and correct copy of the '797 Patent is attached hereto as Exhibit 46.

38. The '797 Patent is generally directed towards computer networks, and more particularly, provides a system to improve the flow of data packets transferring between networks. One of the ways this is accomplished is generating log entries corresponding to the data packets and utilizing the log entries and the packets to correlate the packets transferred between the networks.

39. Centripetal owns by assignment the entire right, title, and interest in and to the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413 Patent, and '797 Patent (collectively, "the Asserted Patents").

40. All of the Asserted Patents are valid and enforceable.

THE ASSERTED PATENTS IMPROVE NETWORK SECURITY

41. Threats to computer network security have grown in number and in sophistication over time. Network security systems, in kind, have to continually improve and become more effective as hackers become increasingly more sophisticated and continue to identify and exploit newfound vulnerabilities. Prior to Centripetal's patented inventions, conventional solutions filtered network traffic in a static manner and thus failed to adequately

meet network security needs in the face of the ever-changing threat landscape. Centripetal's dynamic network security solutions allow network users to implement effective security systems that protect against the latest evolution of network threats.

42. The Asserted Patents are directed to specific improvements in computer network security and more particularly, they are directed to improvements in the way computers analyze network packets and filter these packets to circumvent network threats. A network packet is a fundamental means to transmit data over a computer network. Network packets are specifically formatted in a way that allows computers to communicate over networks by breaking larger messages into discrete chunks that are sent to a destination in the network and then reassembled back into original form at the destination.

43. Network packets are concrete and tangible things in the realm of computer networks because they include pieces of computer files. Operations on network data packets are not something a human could think up in the abstract or with pen and paper. Packets, as used, for example, in the claims of the '028, '126, and '246 Patents, are created for networking and only used in computer networking. The inventions of the Asserted Patents, including the '028, '126 and '246 Patents, are rooted in computer technology and include elements such as computer processors and memory, which are required to process computer network packets.

44. The Asserted Patents, including the inventions claimed in the '028, '126, and '246 Patents discussed further below, are each directed to improved computer network security through a specifically identified solution and cover specific aspects in the field of computer network security.

45. The claims of the '028, '126, and '246 Patents, recite specific, ordered combinations of elements.

46. The ’028 and ’126 Patents share a common specification, which describes how the claimed inventions were an improvement over conventional methods (e.g., analyzing data logs based on the traffic processed by the network devices without regard to the network threat indicators), the use of which were tedious, time consuming, and exacerbated by the continuously evolving nature of potential threats. The claimed inventions of the ’028 and ’126 Patents satisfy the need for rule-based network threat detection by providing methods, devices, and computer readable media that use a rule-based network threat detection technique to improve a computer’s ability to prevent continuously evolving network threats.

47. The ’028 and ’126 Patents are each directed to the use of network threat indicators that are used to prevent malicious attacks on a network. They describe, in detail, that in order to leverage these network threat indicators, the system will apply rules that are based on the network threat indicators and, based on certain conditions, will cause the system to reconfigure the packet filtering device to prevent further traffic into the network. Accordingly, the ’028 and ’126 Patents detail a particular concrete solution, which requires configuring a device to be able to protect a network against malicious attacks occurring worldwide. They go beyond the general idea of improving security, and require specific, unique operations be performed on a particular type of communication (data packets) and particular devices (e.g., modified operators, responsive and updated packet filtering devices).

48. The claimed inventions of the ’028 and ’126 Patents describe many inventive concepts that provide unconventional means for improving network security. Examples include the utilization of information from independent threat intelligence providers and dynamically updating rule sets, which allows network systems to secure their networks with independent information related to the latest threats. Another example is the reconfiguration of operators

within packet filtering rules. Another example is the use of the rule provider device. These improvements permit packet filtering rules to be applied at scale to larger and more complex modern networks. The ’126 Patent claims additionally recite receiving packet filtering rules from a rule provider device, and that the network threat indicators comprise unique Internet host addresses or names.

49. The dependent claims of the ‘028 and ‘126 Patents provides additional technical elements regarding the claimed inventions (e.g., logging, further updating of the packet filtering device, packet flow entry corresponding to the generated packet log entry, specific information and tasks that are generated in response to packet analysis, packet flow logs and ordering of network threats, determining a time or network threat intelligence reports corresponding to network threats, the first portion and second portion of packets).

50. The’246 Patent covers specialized network security devices, methods, and computer readable media that process a high volume of network traffic, on a packet-by-packet basis, with multiple rulesets prioritized to apply different times, allowing the system to effectively protect a network from threats. For example, independent claims 1, 8, and 15 of the ’246 Patent recites steps that describe a specific technique of dynamically forwarding network traffic based on multiple growing rule sets and additionally, include timing requirements of when rule sets are executed. The dependent claims provide additional technical elements regarding the claimed inventions (e.g., encapsulate, multiple packet transformation functions).

51. The inventive concept described in the ’246 Patent of receiving and executing multiple growing rule sets in a specific order is an unconventional means to improve network security and performance. Prior to the inventions of the ’246 Patent, existing reactive and proactive network security solutions were not capable of filtering substantially all network

traffic at a high resolution with a large number of rules. According to the specification, prior to the filing of the '246 Patent, TCP/IP network protocols (e.g., the Transmission Control Protocol (TCP) and the Internet Protocol (IP)), were designed to build large, resilient, reliable, and robust networks, but were not designed with security in mind. Although subsequent developments extended such protocols to provide for secure communication between peers, the networks themselves remained vulnerable to attack. The claims of the '246 Patent recite inventions to address the deficiencies of prior network security systems by looking at a large volume of traffic on a packet-by-packet basis.

52. The inventions of the '246 Patent improve computer security by dynamically utilizing multiple growing rule sets to forward packets through a network. The use of rule sets, which begins with a first rule set which includes a smaller number of network addresses, with additional rule sets which include more network addresses each time, is an innovation which also improves network performance by prioritizing network traffic.

53. As an example, the multiple rule sets may include a first rule set for network traffic that is highest in priority than others (e.g., network traffic for executives of a large corporation), and a subsequent larger rule set for high priority (e.g., network traffic for management, sales, engineers, etc.), and a third even larger rule set for other network traffic (e.g., network traffic for all other users).

54. Traditionally, network traffic would be processed in an opposite manner. For example, rule sets including the largest number of network addresses would be executed first before the smaller number of rule sets. The '246 Patent thus provides inventive and valuable improvements in the security and the efficiency of modern networks.

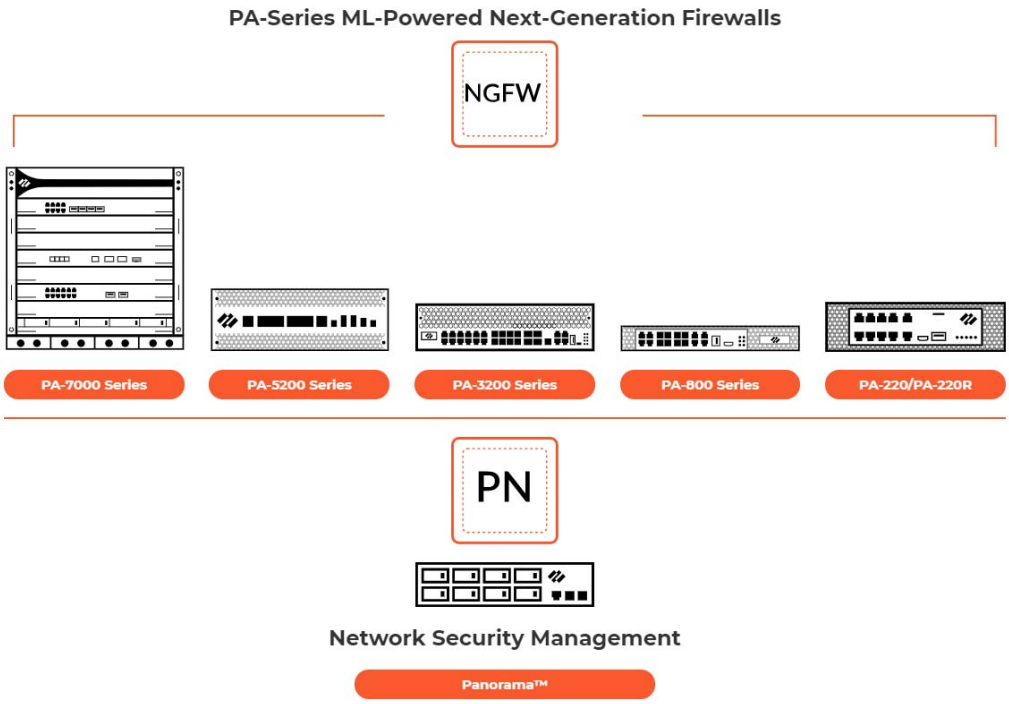
PAN AND ITS PRODUCTS

55. PAN is a multi-billion dollar cybersecurity company that offers security products for enterprise customers. PAN's primary business focuses on computer network security, including through the manufacture and sale of its network security firewalls and related products and services.

56. PAN makes, uses, and sells its Next-Generation Firewall ("NGFW"), a network security product that inspects all traffic, including for applications, threats, and contents. Ex. 14, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/firewall-feature-overview-datasheet. PAN advertises that the NGFW serves as the cornerstone of an effective network security strategy. Ex. 15, https://www.paloaltonetworks.com/resources/whitepapers/firewall-buyers-guide.html. The NGFW relies on shared threat intelligence from multiple sources to provide visibility into known and unknown threats. PAN's current generation of NGFW are machine learning powered to allow its customers to stay ahead of new emerging threats, see and secure their enterprise, and create automated policies that are machine generated. The NGFW leverages machine learning to deliver an inline malware and phishing prevention and to stop unknown threats. The NGFW will automatically reprogram your network with zero-delay signature updates for threats and use telemetry to optimize security policy and eliminate breaches. The NGFW is available in different versions which all perform the same general functions, including as a hardware appliance (PA-Series), a virtual machine (VM-Series), containerized, and cloud-delivered. The NGFW runs the PAN-OS software on hardware components (processors, memory, etc.) and the PAN-OS includes key technologies for visibility and control

of a network, including through implementation of a SD-WAN. Ex. 16, https://docs.paloaltonetworks.com/pan-os.html. The PAN-OS leverages inline machine learning to automatically reprogram your firewall with the latest threat intelligence. Centripetal is informed and believes that PAN released SD-WAN technology in PAN-OS 9.1, which was released on or around December 2019.

57. PAN makes, uses, and sells Panorama, which provides network security management. Ex. 17, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/panorama-centralized-management-datasheet. Panorama allows users to gain insight into network traffic and threats and provision the NGFW with security rules. Panorama allows for the management of network security with a single security rule base that leverages dynamic security updates. Panorama performs automated threat correlation using a predefined set of correlated objects to connect specific hosts to malicious behavior in a network. Panorama is available as a hardware appliance, virtual appliance, and to support cloud services, which all perform the same general functions.



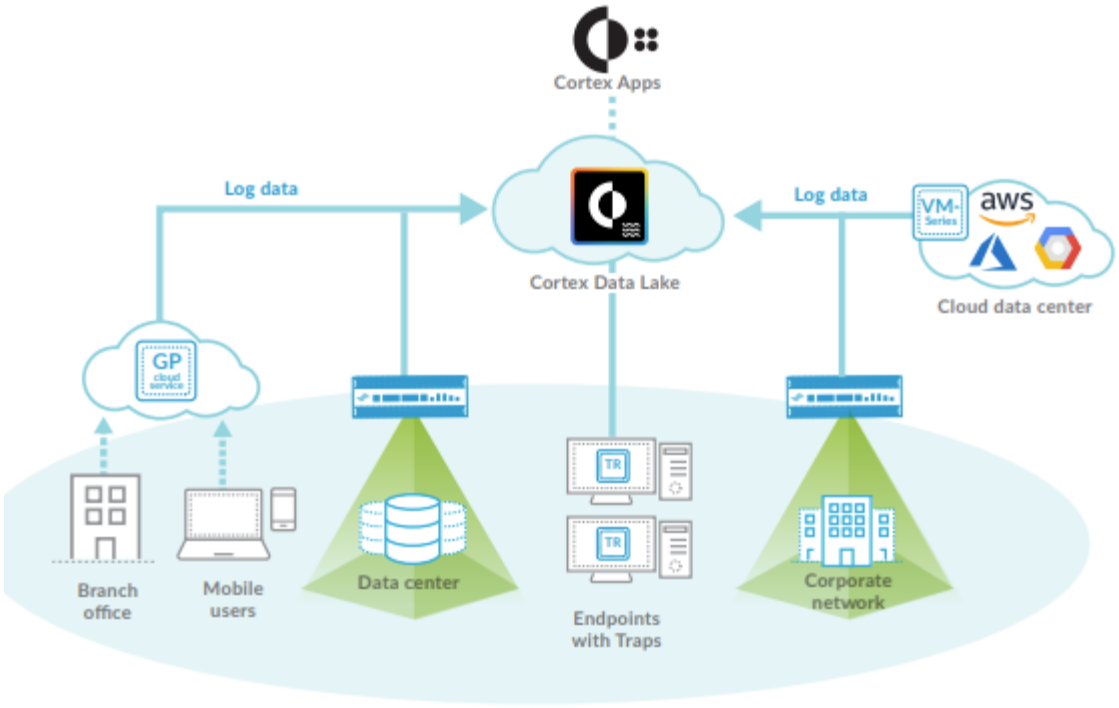
Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

58. PAN makes, uses, and sells Cortex, its artificial intelligence security operations platform. Ex. 19, https://docs.paloaltonetworks.com/cortex.html. Cortex extends next generation security into the cloud and provides a number of different security services that are identified as "Apps" built on Cortex that perform analysis on the Cortex "Data Lake." The Cortex Data Lake stores context-rich enhanced network logs from the PAN security products, such as the NGFW. The Cortex Data Lake allows a customer to collect and analyze expanding volumes of data from a multitude of sources without needing to plan for local computation and storage. Centripetal is informed and believes that PAN began offering Cortex Data Lake on or around March 2018.

59. Apps that are part of Cortex, or utilize the Cortex functionality, include XDR, XSOAR, and AutoFocus. Ex. 19, https://docs.paloaltonetworks.com/cortex.html. Cortex XDR

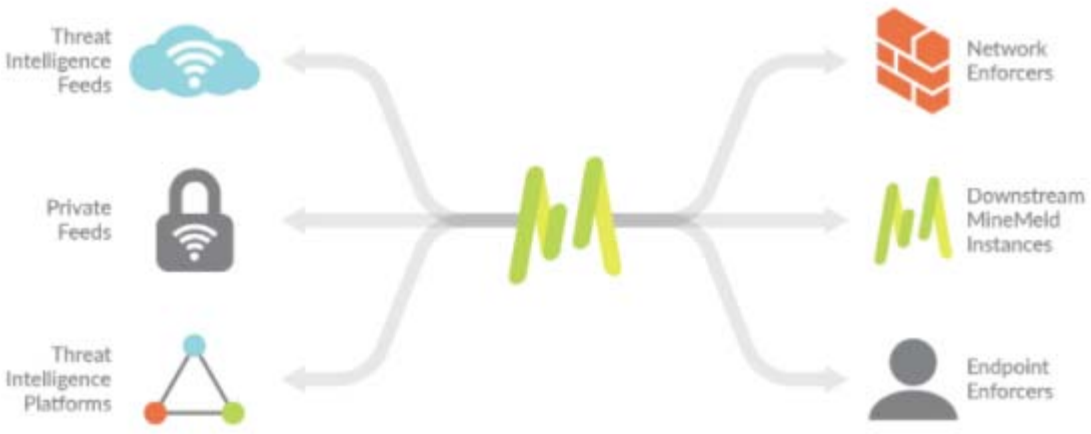
applies machine learning at cloud scale to the rich network, endpoint, and cloud data contained in the Cortex Data Lake to quickly stop security threats. Ex. 20, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-xdr. Cortex XDR automatically detects active attacks allowing them to be contained. Centripetal is informed and believes that PAN began offering Cortex XDR on or around August 2019. Cortex XSOAR combines security orchestration, threat intelligence, and incident management into a single experience. Ex. 21, https://www.paloaltonetworks.com/cortex/xsoar. Cortex XSOAR automates security product tasks by executing automated playbooks, which unify threat intelligence aggregation to allow automated sharing. Centripetal is informed and believes that PAN began offering Cortex XSOAR on or around March 2020. AutoFocus is a cloud-based threat intelligence service that enables the easy identification of attacks so that they can be addressed quickly. Ex. 22, https://docs.paloaltonetworks.com/autofocus.html. AutoFocus correlates threat data from the customer's network and other threat intelligence feeds. Centripetal is informed and believes that AutoFocus was integrated with Cortex (AutoFocus 2.0) on or around November 2019.

60. PAN's Crypsis, a company that PAN acquired in 2020, uses Cortex to protect PAN's customers from cyberattacks and to mitigate the potential impact resulting from a breach. Crypsis improves Cortex's ability to use and generate threat intelligence by strengthening Cortex's ability to collect rich security telemetry, manage breaches, and initiate rapid response actions.



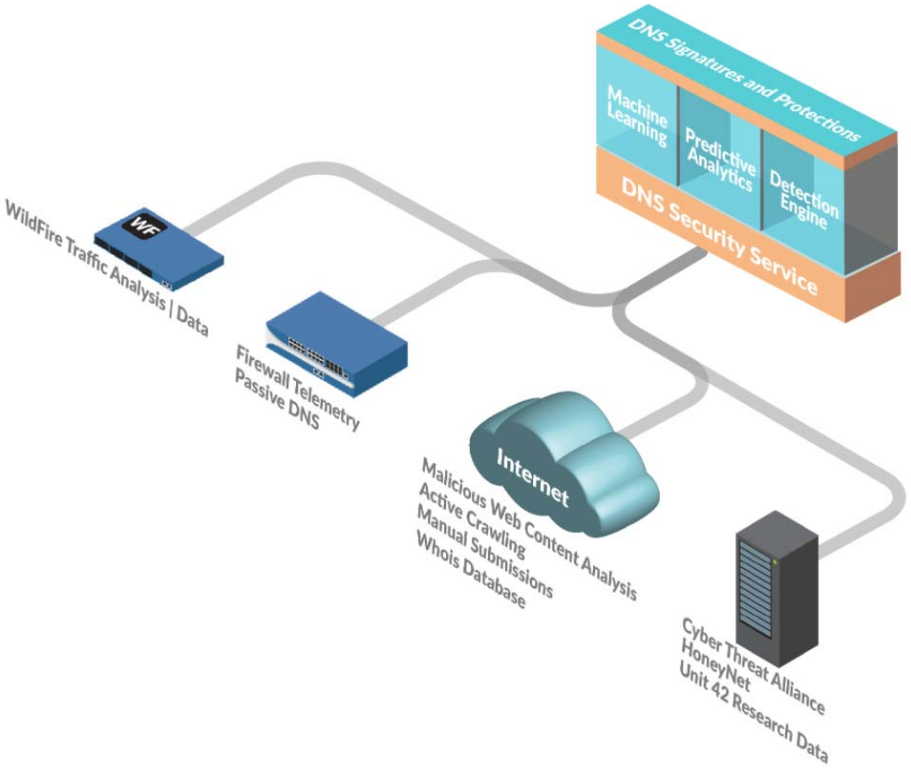
Ex. 23, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

61. PAN's products also integrate with MineMeld, which aggregates and correlates threat intelligence feeds from various threat intelligence providers. Ex. 24, https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld. PAN provides specific instructions and directions to its customers on how to natively integrate MineMeld with its other products and services. MineMeld allows a customer to perform comprehensive analysis and sharing of different feeds. MineMeld natively integrates with PAN products to automatically create new prevention-based controls for URLs, IPs, and domain intelligence. MineMeld integrates with AutoFocus to identify threats and block them on the NGFW. Centripetal is informed and believes that MineMeld was integrated into PAN's products on or around September 2020.



Ex. 24, https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld.

62. PAN makes, uses, and sells its DNS Security Service, which identifies and blocks attacks that use DNS for command-and-control and data theft. Ex. 25, https://www.paloaltonetworks.com/products/threat-detection-and-prevention/dns-security. The DNS Security Service allows for complete visibility into DNS traffic to automate the creation of a sinkhole for malicious domains. Centripetal is informed and believes that DNS Security Service was released by PAN on or around August 2020.



Ex. 26, https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/dns-security/about-dns-security.html#par_concept.

63. PAN also makes, uses, and sells its Enterprise Data Loss Prevention ("DLP") service, which is a cloud delivered data protection service that protects from the exfiltration of sensitive data from a network. Centripetal is informed and believes that PAN began offering Enterprise DLP on or around November 2020.

PAN'S INFRINGEMENT OF CENTRIPETAL'S PATENTS

64. PAN has infringed and continues to infringe one or more claims of each of the Asserted Patents by engaging in acts that constitute infringement under 35 U.S.C. § 271, including but not necessarily limited to making, using, selling, and/or offering for sale, in this district and elsewhere in the United States, and/or importing into this district and elsewhere in

the United States, the accused NGFW, Panorama, Cortex, MineMeld, and/or DNS Security Services alone or in conjunction with one another (collectively, "the Accused Products").

65. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), literally and/or under the doctrine of equivalents, PAN indirectly infringes all the Asserted Patents under 35 U.S.C. §§ 271(b) and (c), literally and/or under the doctrine of equivalents. PAN induces infringement of the Asserted Patents by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to meet claim elements, literally and/or under the doctrine of equivalents, of the Asserted Patents. PAN contributorily infringes the Asserted Patents by making and supplying products that are components in an infringing system with components from manufacturers, customers, purchasers, users, and developers that together meet all claim elements in the Asserted Patents, literally and/or under the doctrine of equivalents. Centripetal is informed and believes that PAN had knowledge of the Asserted Patents prior to its initial Complaint filed on March 12, 2021, and at the very least, has become aware of its infringement of the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413 Patent as of the initial Complaint filed on March 12, 2021, and aware of its infringement of the '797 Patent as of being served with this Amended Complaint on June 30, 2021.

66. Centripetal's products and services are marked with Centripetal's patents. For example, Centripetal's products and services have been marked with the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413, and '797 Patent, upon their issuance. In addition, Centripetal's public website and product datasheets identify that Centripetal has issued and

pending patents, and its website includes a list of patent numbers, in compliance with 35 U.S.C. § 287. Ex. 27, https://www.centripetal.ai/legal?__hstc=98722881.83379b6542bff476abf41ef99a471a87.1613070891083.1613070891083.1614036867078.2&__hssc=98722881.1.1614036867078&__hsfp=2496945082.

67. Centripetal is informed and believes that PAN had knowledge of the Asserted Patents based on PAN's interactions with Centripetal through various channels, including acquiring knowledge of patents by way of Centripetal's marking of its products. Despite its knowledge of Centripetal's patent rights, PAN engaged in willful infringement and egregious behavior warranting enhanced damages.

68. Since 2014, PAN has visited Centripetal's website hundreds of times and has visited numerous pages on Centripetal's website regarding business, products, patents, and press releases discussing Centripetal's patent litigations against Keysight Technologies, Inc. Ixia, and Cisco Systems, Inc. By downloading materials from Centripetal's website and by correspondence with Centripetal, PAN's engineers, business development, and sales employees have received and reviewed datasheets and white papers regarding Centripetal's products. Centripetal's datasheets indicate Centripetal's products are subject to one or more U.S. patents.

69. In late May 2016, Shea & Company, an investment bank, introduced Centripetal to PAN's Sr. Director of Business and Corporate Development, to discuss a potential partnership between the two companies. In early and mid-June 2016, several Centripetal employees, including Centripetal's CEO and Founder, had several telephone conversations with members of PAN's Business and Corporate Development team to explore the possibility of PAN being a threat intelligence partner. In e-mail correspondence exchanged with PAN in

June 2016, Centripetal provided an overview of its technology and provided industry publications on the importance of threat intelligence gateways and Centripetal's patented technology.

70. After these initial communications, PAN requested additional information regarding Centripetal's product offerings and technology. On June 21, 2016, Centripetal and PAN executed a mutual Non-Disclosure Agreement ("NDA") to protect disclosure of exchanged confidential information. Upon executing the NDA, Centripetal disclosed details to about its proprietary patented technology and confidential details about, *inter alia*, how Centripetal's technical solution works, why it works, why it is effective and its strategic business strategies in the marketplace for its technical solution. Despite showing interest in order to get access to Centripetal's confidential and proprietary information, PAN thereafter indicated that it was not interested in doing business with Centripetal, and did not follow up any further regarding a potential partnership with Centripetal.

71. Since 2016, Centripetal has met with PAN employees at several industry conferences including the RSA conference, Gartner Security Conference, and International Quality and Productivity Center (IQPC) conference. Centripetal provided demonstrations of its products at these industry conferences.

72. In July 2017, Oppenheimer, an investment banker, reached out to PAN to introduce Centripetal as an investment opportunity. PAN's Senior Vice-President of Business and Corporate Development expressed interest in talking to Centripetal and suggested the two companies schedule a more detailed technical discussion with PAN's creator and lead developer of Minemeld, Mr. Mori. As the parties had already signed an NDA, on August 7, 2017, Centripetal's founder and CEO, Steven Rogers, discussed with Mr. Mori how to

integrate Centripetal's technology with PAN's existing products. Mr. Mori requested access to technical documentation regarding Centripetal's products. During the call, Mr. Mori stated that PAN did not have any technology that could scale like Centripetal's technology, and was interested in how Centripetal's technology could interface with PAN's.

73. Centripetal is informed and believes that PAN has also been aware of Centripetal's Asserted Patents through other publicly available information, including published patent applications for the Asserted Patents and prior patent litigations filed by Centripetal against PAN competitors, Keysight Technologies, Inc. Ixia, and Cisco Systems, Inc. in 2017 and 2018 respectively, where the asserted patents are in the same families as the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '906 Patent, '246 Patent, '413, and '797 Patent in this action, and the accused Keysight and infringing Cisco products are competitive with the PAN Accused Products. Publicly available information before the date of Centripetal's initial Complaint of March 12, 2021, including from the U.S. Patent and Trademark Office, identifies the applications for the Asserted Patents as being related to the patents asserted against Cisco and Keysight. On information and belief, PAN has been aware, based on publicly available information, that Centripetal settled with Keysight in 2019, and obtained a judgment of validity and infringement against Cisco in October 2020 and damages of $2.6 to $3.2 billion based on a 5-10% royalty rate.

74. Centripetal is informed and believes that PAN was aware of the Asserted Patents, and has done nothing to curtail its infringement.

75. Centripetal is informed and believes that despite PAN's knowledge of the Asserted Patents and Centripetal's patented technology, PAN made the deliberate decision to sell products and services that it knew infringes Centripetal's Asserted Patents.

76. Centripetal is informed and believes that PAN has undertaken no efforts to avoid infringement of the Asserted Patents, despite PAN's knowledge and understanding that PAN's products and services infringe these patents. Thus, PAN's infringement of Asserted Patents is willful and egregious, warranting enhancement of damages.

77. Centripetal is informed and believes that PAN knew or was willfully blind to Centripetal's patented technology. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

FIRST CAUSE OF ACTION
(Direct Infringement of the '028 Patent pursuant to 35 U.S.C. § 271(a))

78. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

79. PAN has infringed and continues to infringe a least Claims 1-3, 5-10, 12-17, and 19-21 of the '028 Patent.

80. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

81. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

82. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the

‘028 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Panorama, Cortex, AutoFocus, MineMeld, and/or DNS Security Service (the “’028 Accused Products”). Combinations of the ‘028 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the ‘028 Accused Products infringe under at least the following scenarios: (1) NGFW, (2) NGFW and Panorama, (3) NGFW, Panorama, and Cortex, (4) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus, MineMeld or DNS Security. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

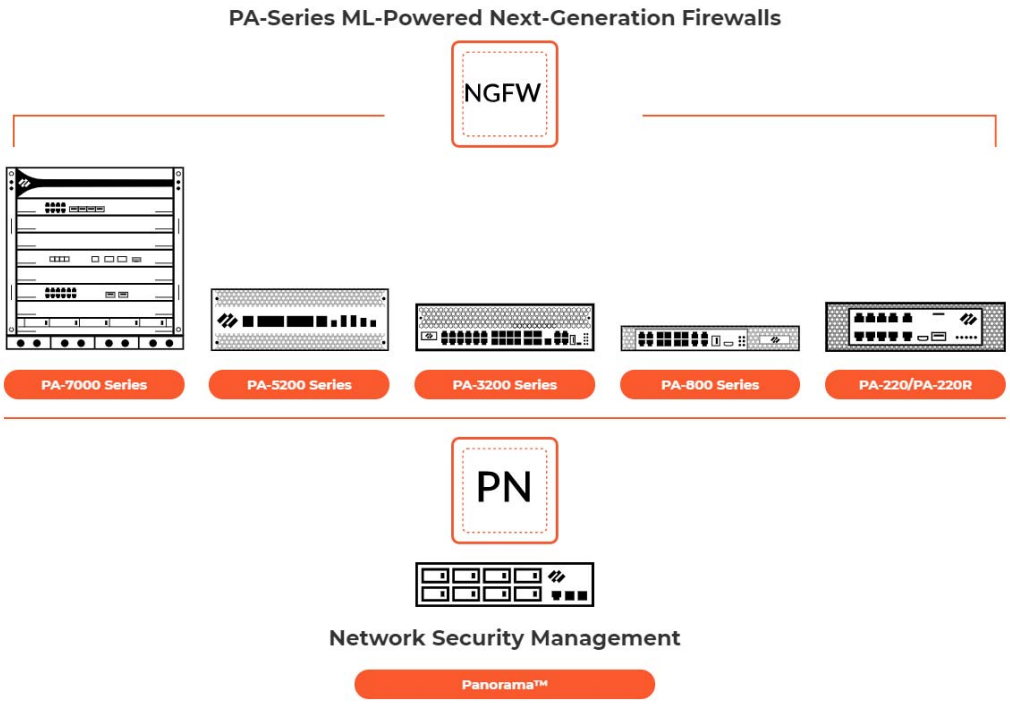
83. The ‘028 Accused Products embody the patented invention of the ‘028 Patent and infringe the ‘028 Patent because they include a packet filtering device with at least one processor; and memory comprising instructions that, when executed by the at least one processor, cause the packet filtering device to: receive a plurality of packet filtering rules configured to cause the packet filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators, wherein the plurality of network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers; receive a plurality of packets that comprises a first packet and a second packet; responsive to a determination that the first packet satisfies a first packet filtering rule, of the plurality of packet filtering rules, based on one or more network-

threat indicators, of the plurality of network-threat indicators, specified by the first packet filtering rule: apply, to the first packet, an operator specified by the first packet filtering rule and configured to cause the packet filtering device to allow the first packet to continue toward a destination of the first packet; and communicate information that identifies the one or more network-threat indicators and data indicative that the first packet was allowed to continue toward the destination of the first packet; receive an update to at least one packet filtering rule; modify, based on the received update to the at least one packet filtering rule, at least one operator specified by the first packet filtering rule to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations; and responsive to a determination that the second packet satisfies the first packet filtering rule: based on the modified at least one operator specified by the first packet filtering rule, prevent the second packet from continuing toward a destination of the second packet; and communicate data indicative that the second packet was prevented from continuing toward the destination of the second packet.

84. The ‘028 Accused Products are packet security gateways which protect large organizations, data centers, and high bandwidth network perimeters. The ‘028 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that stores instructions to be executed by the memory.

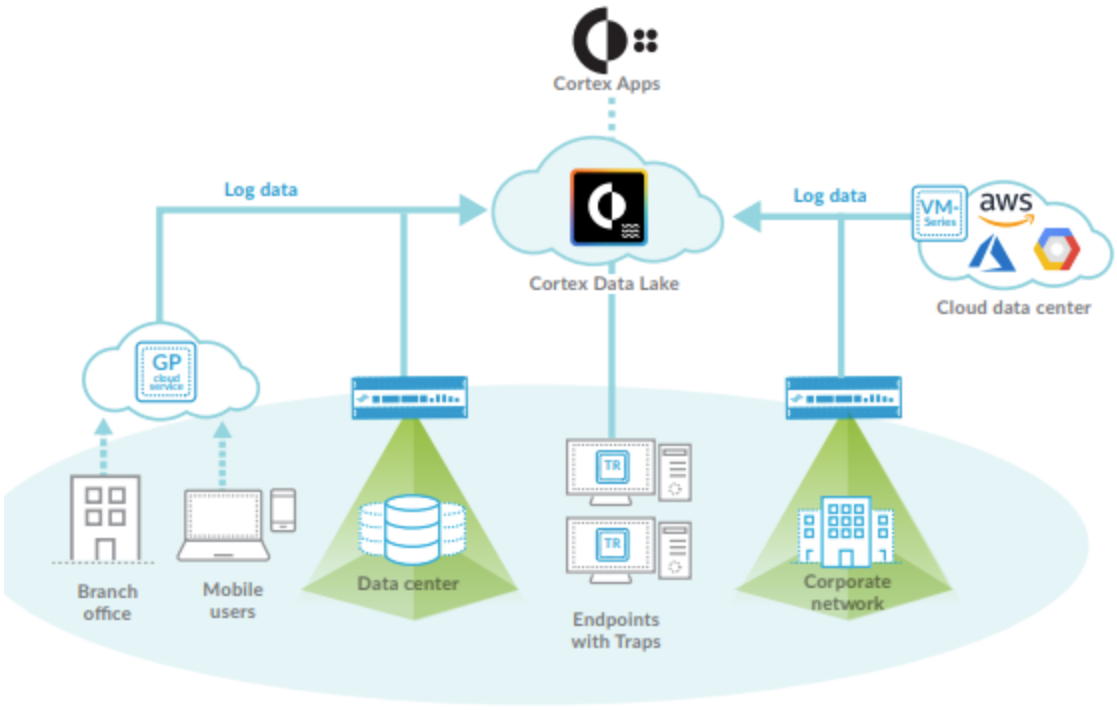
85. For example, with the ‘028 Accused Products, the NGFW receives packet filtering rules, one of which is a “first packet filtering rule,” from Panorama, which is a rule provider device. The DSP includes packet filtering rules, one of which is a “first packet filtering rule,” applied to all traffic traversing the network boundary. Panorama acts as a centralized security management system for global control of the NGFW and provides a single

security rule base for threat prevention, URL filtering, application awareness, user identification, and sandboxing. The packet filtering rules received by NGFW from Panorama are applied to all traffic traversing the network boundary. For example, Panorama, through AutoFocus, provides integrated logs, malware analysis reports, and visibility into malicious events. AutoFocus threat feeds include IP addresses, domains, URLs, and hash indicators that are updated daily and form the packet filtering rules. AutoFocus is a threat intelligence analysis database that creates rules which are provisioned to the NGFW using MineMeld and form the packet filtering rules. Additionally, Panorama provides threat intelligence and network security management using AutoFocus contextual threat intelligence, Cortex (including XSOAR and XDR), that form packet filtering rules. These packet filtering rules include operators which specify whether the particular packets should be blocked or allowed. The operators can be updated, and therefore modified, based on packet filtering rule updates, which can specify whether to block or allow the packet.



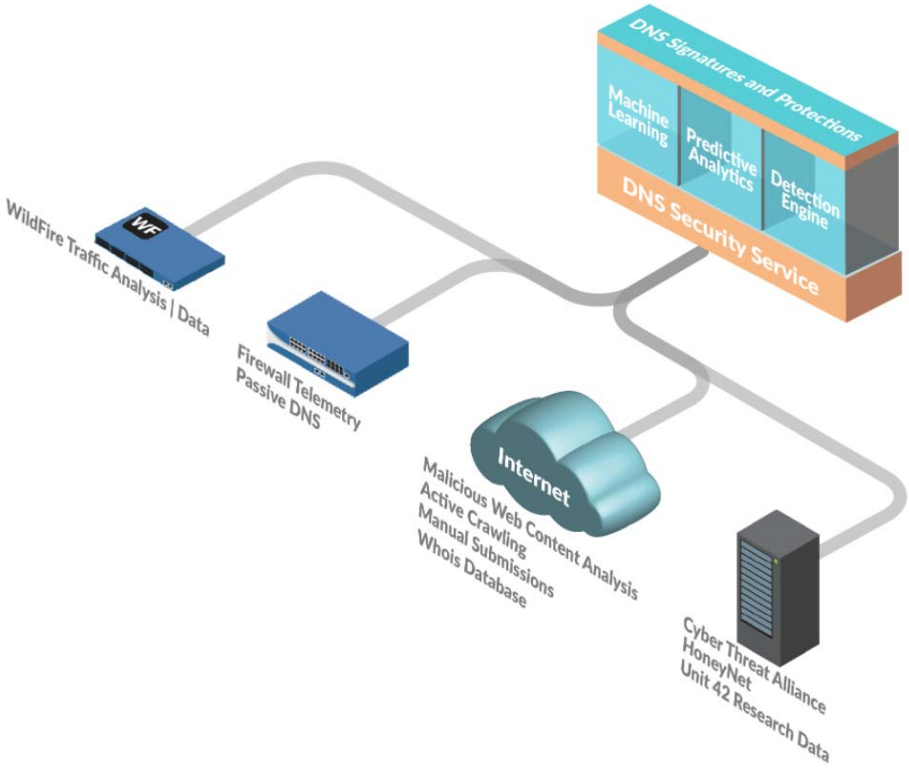
Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

86. As an additional example, the NGFW receives packet filtering rules from Cortex, which is a rule provider device. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers. Shown below, Cortex XDR analyzes network data with machine learning, to pinpoint targeted attacks, malicious insiders and compromised endpoints, and form the packet filtering rules. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers.



Ex. 23, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

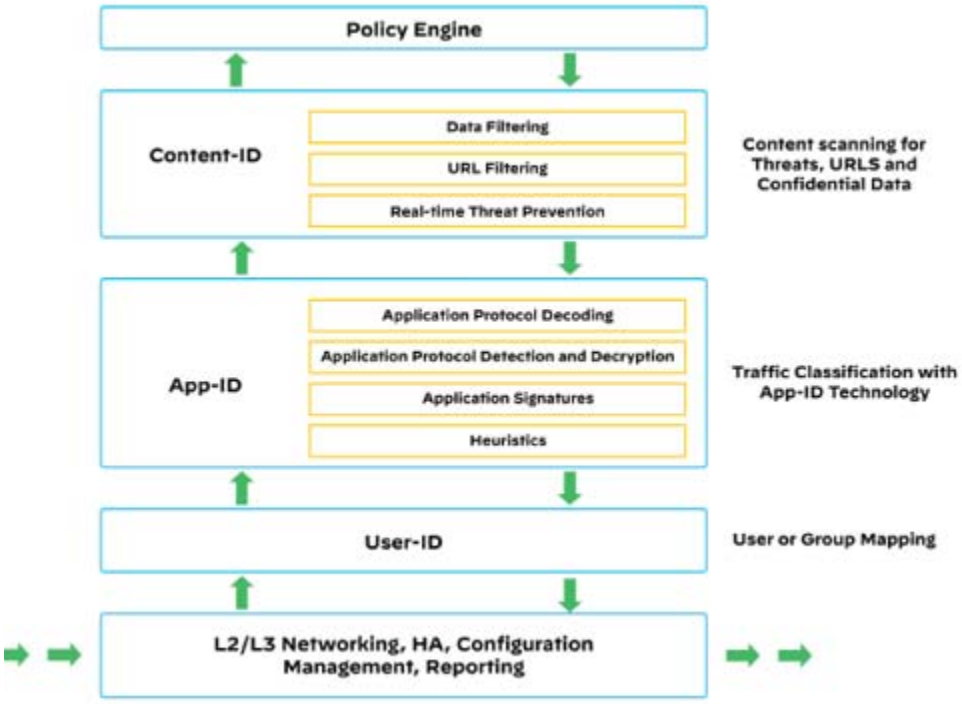
87. Furthermore, the NGFW includes DNS Security Service, which protects and defends from advanced threats using DNS, which leverages advanced machine learning and predictive analytics, to provide real-time DNS request analysis and rapid production of DNS signatures specifically designed to defend against malware using DNS for C2 and data theft. In this way, it provides access to a threat intelligence system to keep network protections up to date.



Ex. 26, https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/dns-security/about-dns-security.html#par_concept.

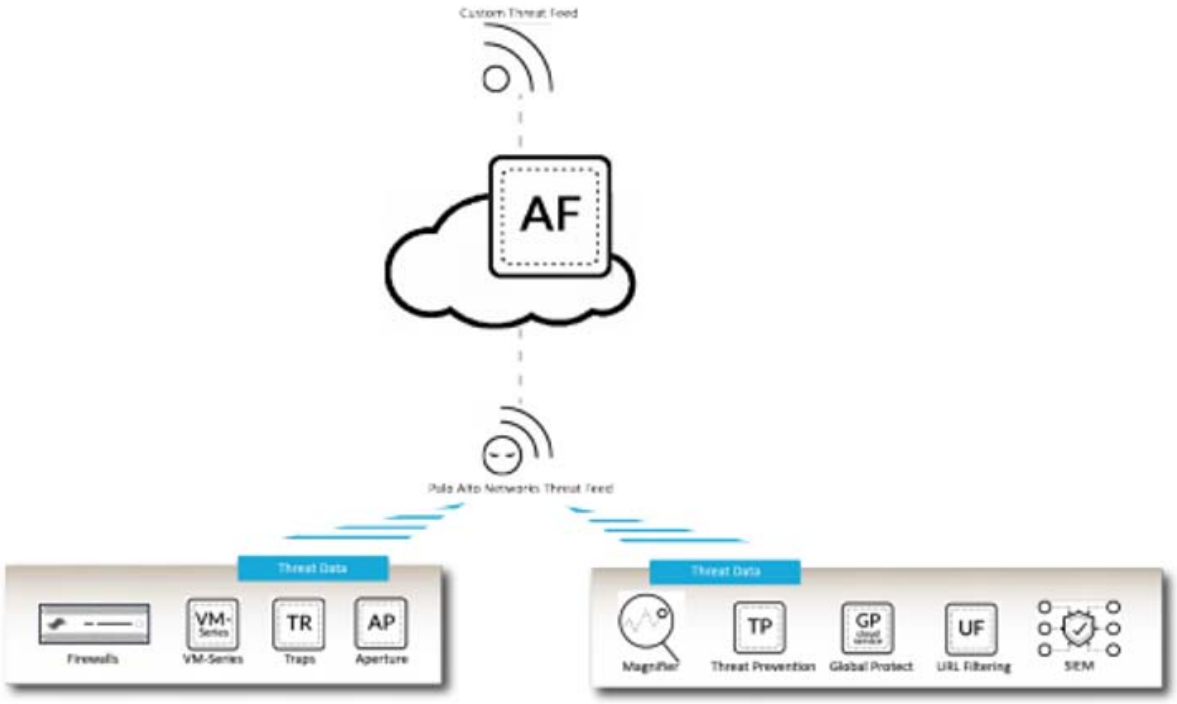
88. The '028 Accused Products use a single-pass architecture, to process each packet, including with policy lookup, decoding, threat detection, content checking, application checking, and networking. The NGFW uses security policy rules as packet-filtering rules and applies them to bidirectional traffic, including inbound and outbound packets. The NGFW is

also zone-based and segments where all nodes share similar network security requirements and evaluates traffic as it passes from one zone to another. The NGFW, with an operator, performs packet processing using rules from various policies, including the Security Policy Lookup to allow or deny packets. The NGFW includes DNS Security, which analyzes network packets to determine the packet satisfies the packet filtering rules, such as the DNS Security rules. You can then capture packets for further analysis.



Ex. 29 at 14, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

89. In the '028 Accused Products, information is communicated to Panorama, including whether packets were allowed or blocked. In a further example, Panorama includes AutoFocus threat feeds, which include IP addresses, domains, URLs, and hash indicators that are updated based on the most recent threat information, which can include updating network threat indicators based on the latest threat information. After this update occurs, the '028 Accused Product is updated to operate on subsequent packets with the packet filtering rule.



Ex. 30 at 165, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/autofocus/autofocus-admin/autofocus-admin.pdf.

90. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

91. PAN has willfully infringed the '028 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '028 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

92. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '028 Patent.

93. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

94. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '028 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '028 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously in infringement of the '028 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

95. PAN's infringement of the '028 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

96. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

97. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SECOND CAUSE OF ACTION
(Indirect Infringement of the '028 Patent)

98. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

99. PAN has induced and continues to induce infringement of one or more claims of the '028 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '028 Patent under 35 U.S.C. § 271(c).

100. PAN has induced infringement of the '028 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more components of a system or computer-readable medium claim, either literally or under the doctrine of equivalents. All the elements of the claims are used by either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '028 Patent, including Claims 1-3, 5-10, 12-17, and 19-21.

101. PAN has knowingly and actively aided and abetted the direct infringement of the '028 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '028 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '028 Patent and how they are intended to be used, as described above and incorporated by reference here. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '028 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '028 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '028 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits

from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

102. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '028 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '028 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

103. PAN contributorily infringes the '028 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '028 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '028 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '028 Patent, including Claims 1-3, 5-10, 12-17, and 19-21.

104. PAN has knowingly and actively contributed to the direct infringement of the '028 Patent by its manufacture, use, offer to sell, sale and importation of the '028 Accused

Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '028 Patent, as described above and incorporated by reference here. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

105. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

106. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '028 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '028 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '028 Patent.

107. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

THIRD CAUSE OF ACTION
(Direct Infringement of the '126 Patent pursuant to 35 U.S.C. § 271(a))

108. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

109. PAN has infringed and continues to infringe a least Claims 1-2, 4-6, 8-9, 11-13, 15-16, and 18-20 of the '126 Patent.

110. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

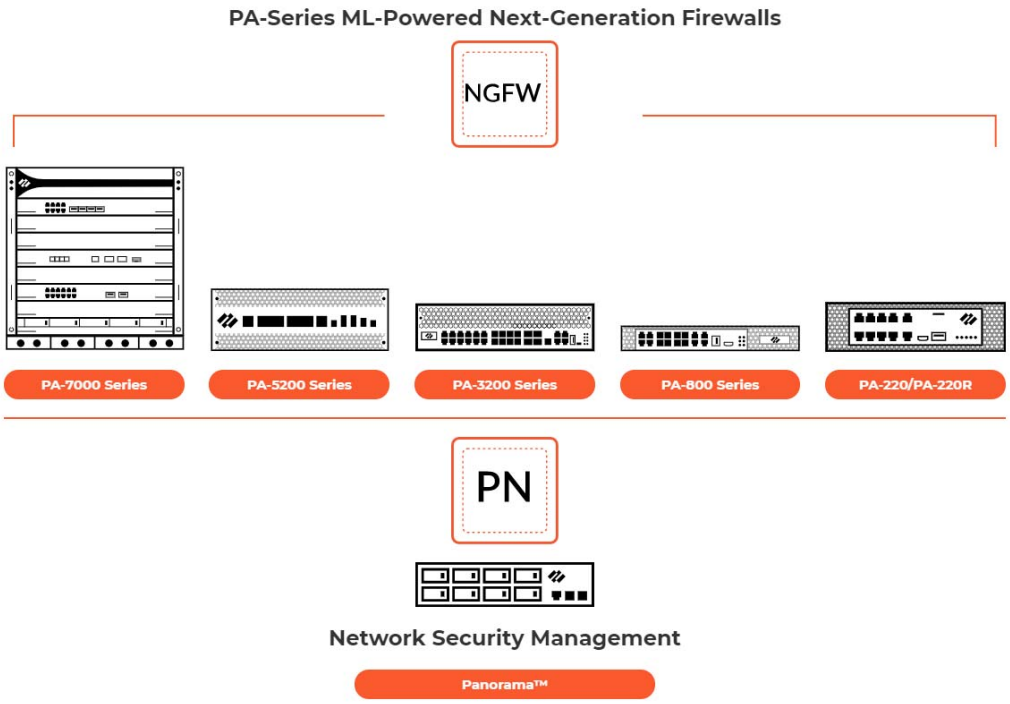
111. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

112. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '126 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Panorama, Cortex, AutoFocus, MineMeld, and/or DNS Security Service (the "'126 Accused Products"). Combinations of the '126 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '126 Accused Products infringe under at least the following scenarios: (1) NGFW, (2) NGFW and Panorama, (3) NGFW, Panorama, and Cortex, (4) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus, MineMeld or DNS Security. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

113. The '126 Accused Products embody the patented invention of the '126 Patent and infringe the '126 Patent because they include a packet filtering device with one or more processors; and memory storing instructions that, when executed by the one or more processors, cause the packet filtering device to: receive, from a rule provider device, a plurality of packet filtering rules configured to cause the packet filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators, wherein the plurality of packet filtering rules were generated by the rule provider device based on network threat intelligent reports supplied by one or more independent network-threat-intelligence providers, and wherein the plurality of network-threat indicators comprise unique Internet host addresses or names; responsive to a determination that a first packet satisfies a first packet filtering rule of the plurality of packet filtering rules based on one or more network-threat indicators specified by the first packet filtering rule: apply, to the first packet, an operator specified by the first packet filtering rule and configured to cause the packet filtering device to allow the first packet to continue toward a destination of the first packet; and communicate, to the rule provider device, data indicative that the first packet was allowed to continue toward the destination of the first packet; receive, from the rule provider device, an update to at least one packet filtering rule; modify, based on the received update to the at least one packet filtering rule, the first packet filtering rule to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations; and responsive to a determination that a second packet satisfies the modified first packet filtering rule: prevent, based on at least one operator specified by the modified first packet filtering rule, the second packet from continuing toward a destination of

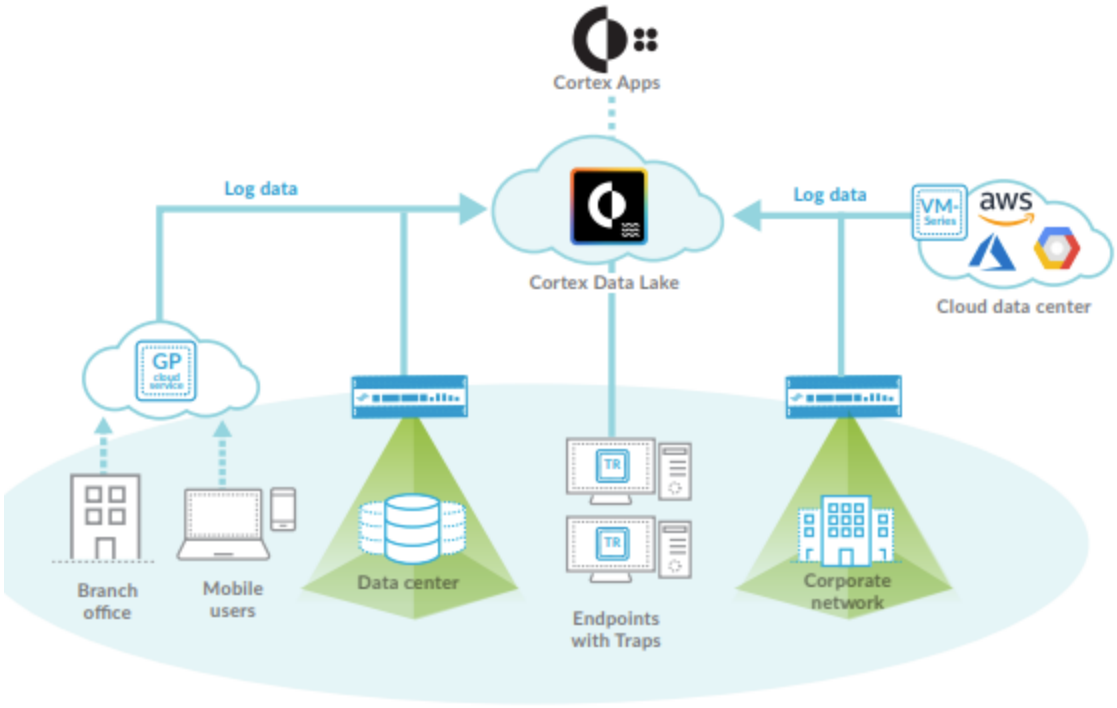
the second packet; and communicate, to the rule provider device, data indicative that the second packet was prevented from continuing toward the destination of the second packet.

114. For example, with the '126 Accused Products, the NGFW receives plurality of packet filtering rules, one of which is a "first packet filtering rule," from Panorama, which is a rule provider device. The packet filtering rules are applied to all traffic traversing the network boundary. Panorama acts as a centralized security management system for global control of the NGFW and provides a single security rule base for threat prevention, URL filtering, application awareness, user identification, and sandboxing. The packet filtering rules are applied to all traffic traversing the network boundary. For example, Panorama, through AutoFocus, provides integrated logs, malware analysis reports, and visibility into malicious events. AutoFocus threat feeds include IP addresses, domains, URLs, and hash indicators that are updated daily and form the packet filtering rules. AutoFocus is a threat intelligence analysis database creates rules which are provisioned to the NGFW using MineMeld and form the packet filtering rules. Additionally, Panorama provides threat intelligence and network security management using AutoFocus contextual threat intelligence, Cortex (including XSOAR and XDR), that form packet filtering rules. These packet filtering rules include operators which specify whether the particular packets should be blocked or allowed. The operators can be updated, and therefore modified, based on packet filtering rule updates, which can specify whether to block or allow the packet. The packet filtering rules reconfigure the NGFW to process packets in a particular manner, such as preventing or allowing the packets.



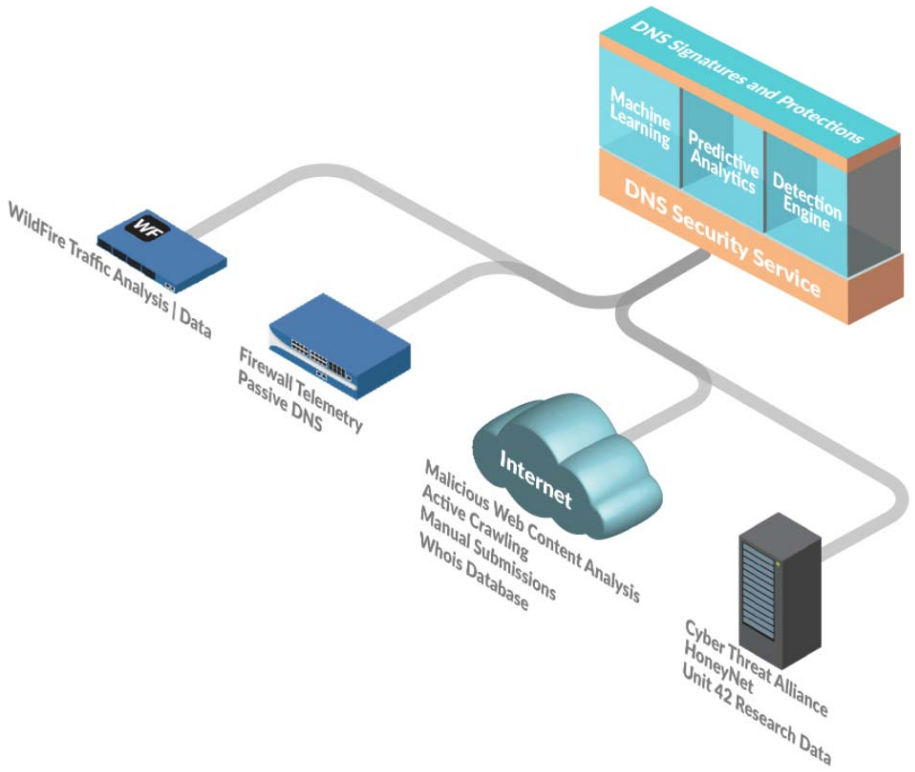
Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

115. As an additional example, the NGFW receives packet filtering rules from Cortex, which is a rule provider device. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers. Shown below, Cortex XDR analyzes network data with machine learning, to pinpoint targeted attacks, malicious insiders and compromised endpoints, and form the packet filtering rules. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers.



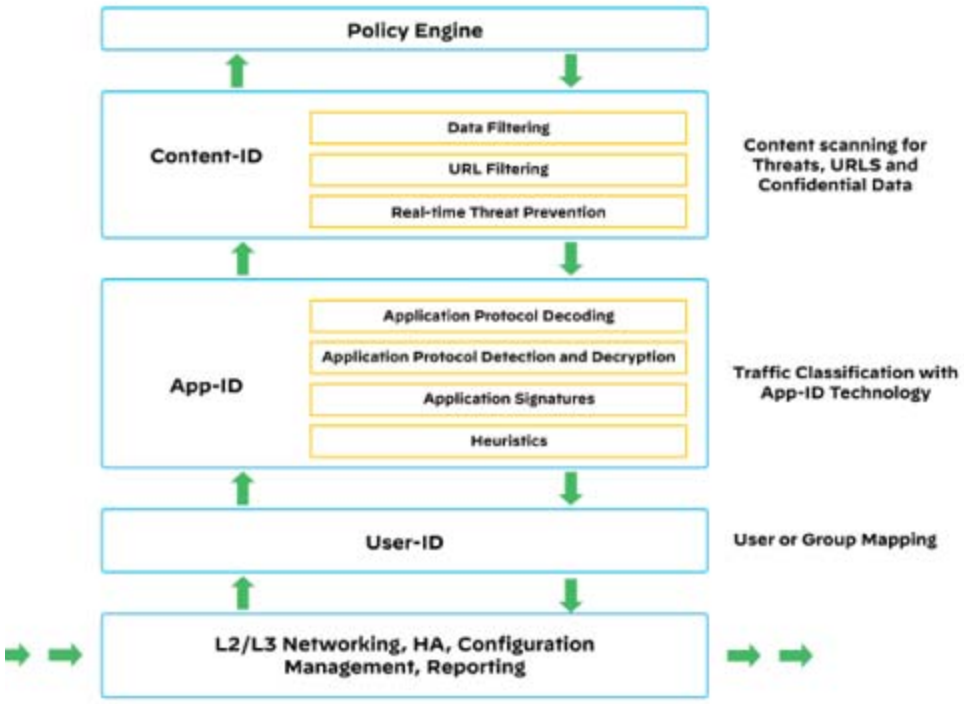
Ex. 23, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

116. Furthermore, the NGFW includes DNS Security Service, which protects and defends from advanced threats using DNS, which leverages advanced machine learning and predictive analytics, to provide real-time DNS request analysis and rapid production of DNS signatures specifically designed to defend against malware using DNS for C2 and data theft. In this way, it provides access to a threat intelligence system to keep your network protections up to date.



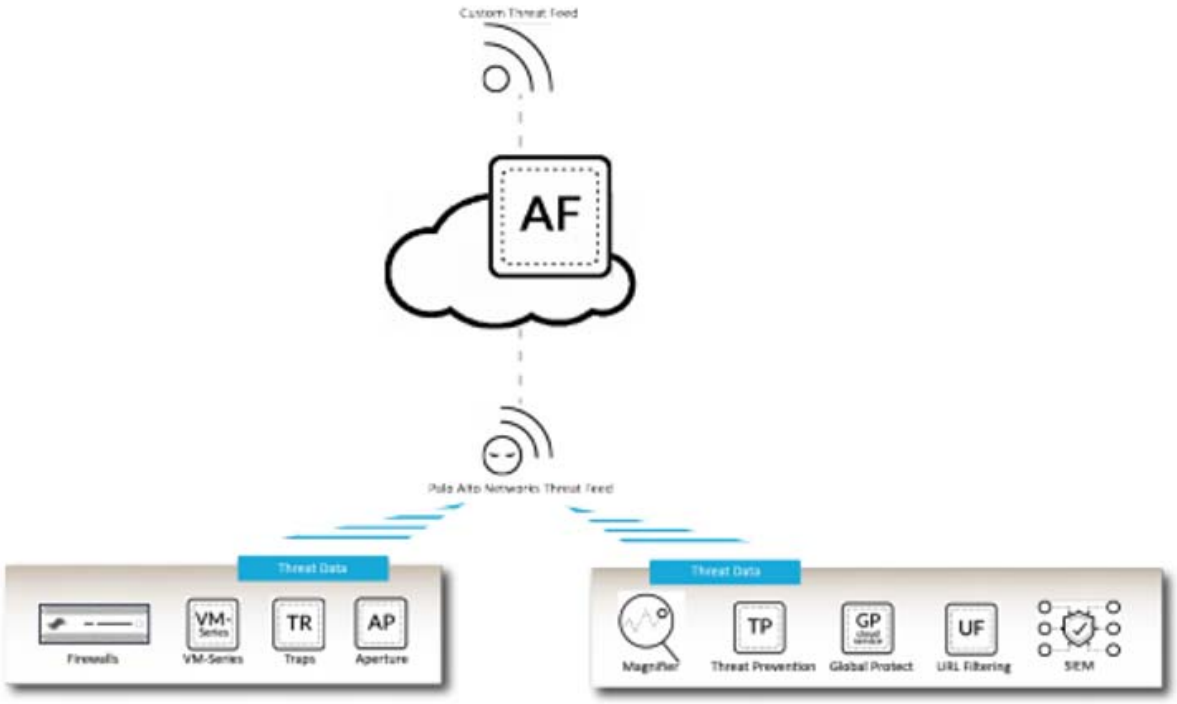
Ex. 26, https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/dns-security/about-dns-security.html#par_concept.

117. The '126 Accused Products use a single-pass architecture, to process each packet, including with policy lookup, decoding, threat detection, content checking, application checking, and networking. The NGFW uses security policy rules as packet-filtering rules and applies them bidirectional traffic, including inbound and outbound packets. The NGFW is also zone-based and segments where all nodes share similar network security requirements and evaluate traffic as it passes from one zone to another. The NGFW, with an operator, performs packet processing using rules from various policies, including the Security Policy Lookup to allow or deny packets. The NGFW includes DNS Security, which analyzes network packets to determine the packet satisfies the packet filtering rules, such as the DNS Security rules. You can then capture packets for further analysis.



Ex. 29 at 14, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

118. In the '126 Accused Products, information is communicated to Panorama, including whether packets were allowed or blocked. In a further example, Panorama includes AutoFocus threat feeds, which include IP addresses, domains, URLs, and hash indicators that are updated based on the most recent threat information, which can include updating network threat indicators based on the latest threat information. After this update occurs, the '126 Accused Products is updated to operate on subsequent packets with the packet filtering rule.



Ex. 30 at 165, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/autofocus/autofocus-admin/autofocus-admin.pdf.

119. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

120. PAN has willfully infringed the '126 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '126 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

121. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '126 Patent.

122. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

123. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '126 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '126 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '126 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

124. PAN's infringement of the '126 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

125. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

126. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FOURTH CAUSE OF ACTION
(Indirect Infringement of the '126 Patent)

127. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

128. PAN has induced and continues to induce infringement of one or more claims of the '126 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '126 Patent under 35 U.S.C. § 271(c).

129. PAN has induced infringement of the '126 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '126 Patent, including Claims 1-2, 4-6, 8-9, 11-13, 15-16, and 18-20.

130. PAN has knowingly and actively aided and abetted the direct infringement of the '126 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '126 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '126 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '126 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '126 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '126 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users,

developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

131. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '126 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '126 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

132. PAN contributorily infringes the '126 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '126 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '126 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '126 Patent, including Claims 1-2, 4-6, 8-9, 11-13, 15-16, and 18-20.

133. PAN has knowingly and actively contributed to the direct infringement of the '126 Patent by its manufacture, use, offer to sell, sale and importation of the '126 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or

vendors to meet the elements of the '126 Patent as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

134. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

135. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '126 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '126 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '126 Patent.

136. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FIFTH CAUSE OF ACTION
(Direct Infringement of the '903 Patent pursuant to 35 U.S.C. § 271(a))

137. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

138. PAN has infringed and continues to infringe a least Claims 1-8 and 10-17 of the '903 Patent.

139. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

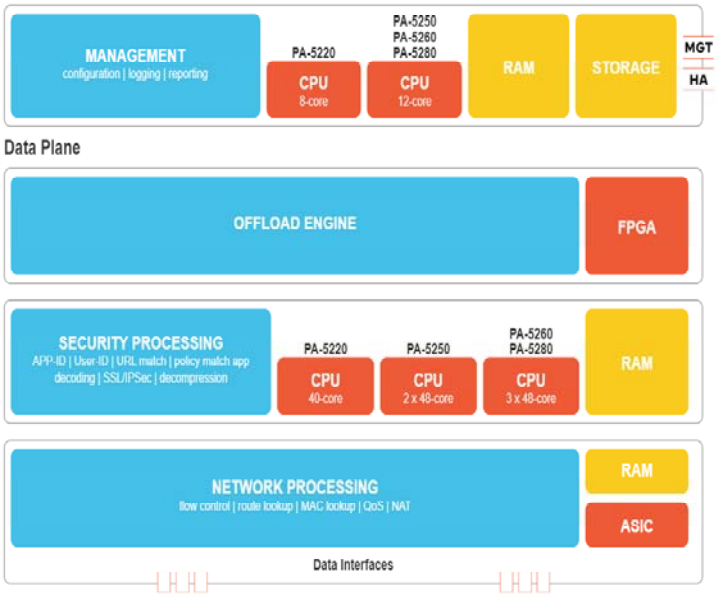
140. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

141. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '903 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW and/or Cortex (the "'903 Accused Products"). Combinations of the '903 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, NGFW and Cortex, separately or in combination, infringe the '903 Patent. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

142. The '903 Accused Products embody the patented invention of the '903 Patent and infringe the '903 Patent because they determine, by a computing system, that a network device has received, from a first host located in a first network, a plurality of first packets corresponding to first requests for content from a second host located in a second network,

wherein the network device comprises a proxy; determine, by the computing system, that the network device has generated a plurality of second packets corresponding to second requests, wherein the second requests correspond to the first requests, and wherein the second requests are configured to cause the second host to transmit, to the network device, the content; generate, by the computing system, a first plurality of log entries corresponding to the plurality of first packets, wherein each of the first plurality of log entries comprises a receipt timestamp indicating a packet receipt time, and wherein the first plurality of log entries comprise first data from the first requests; generate, by the computing system, a second plurality of log entries corresponding to a plurality of second packets, wherein each of the second plurality of log entries comprises a transmission timestamp indicating a packet transmission time, and wherein the second plurality of log entries comprise second data from the second requests; determine, by the computing system and for each transmission timestamp, differences between at least one packet transmission time indicated by transmission timestamps and at least one packet receipt time indicated by receipt timestamps; correlate, based on the differences and by comparing the first data and the second data, at least a portion of the plurality of first packets and at least a portion of the plurality of second packets; and responsive to the correlating: generate, by the computing system, an indication of the first host and transmit, by the computing system, the indication of the first host.

143. For example, as shown below, the ’903 Accused Products include at least one processor and memory comprising instructions that, when executed by the at least one processor, cause a computing device to perform functionalities.



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

144. For instance, Cortex XDR is used to "[d]etect targeted attacks, insider threats, and malware with AI-powered analytics" and "monitor internet traffic as well as internal, east-west communications between your users and servers to detect post-intrusion activity, such as lateral movement and exfiltration."

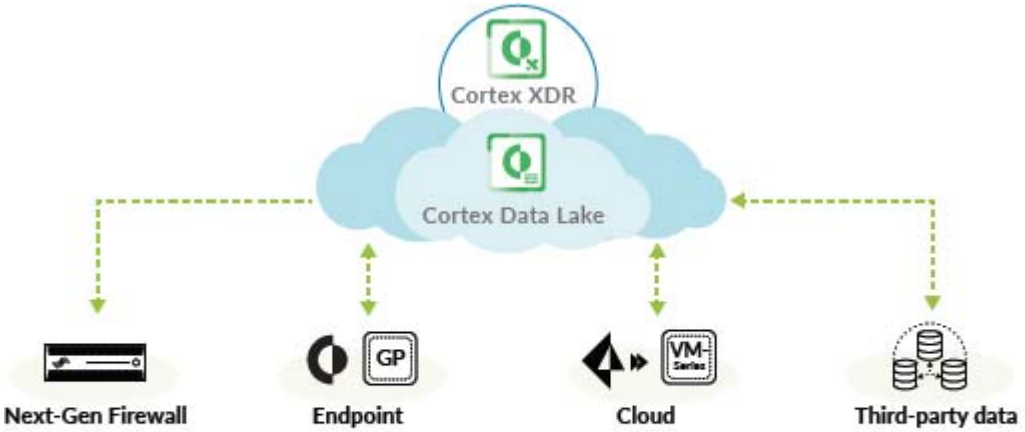


Figure 2: Cortex XDR with one or more data sources for detection and response, eliminating blind spots

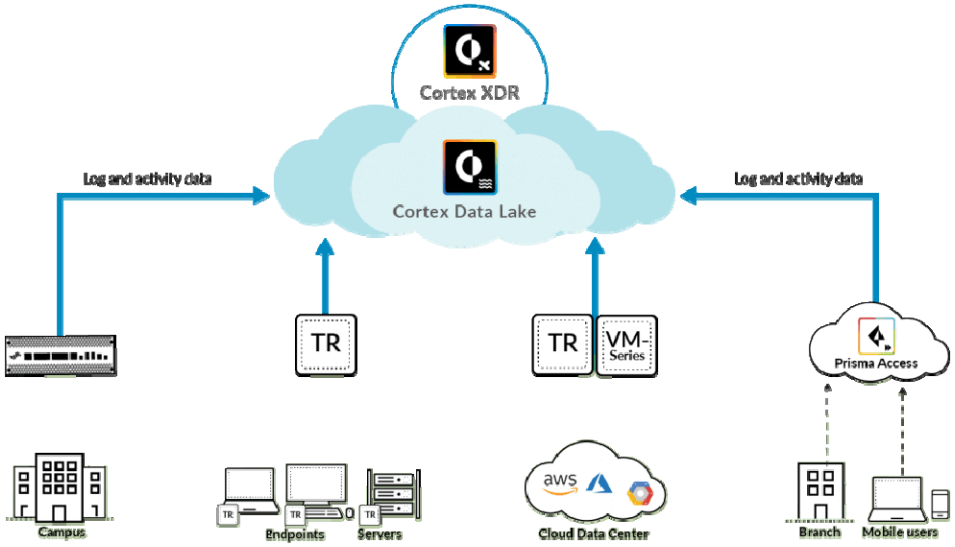
Ex. 32 at 1-2,

https://live.paloaltonetworks.com/twzvq79624/attachments/twzvq79624/members_discuss/84686/1/Cortex_XDR-NTA.pdf;

Ex. 33 at 26,

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf.

145. The NGFW generates log and activity data which are collected and stored in the cloud-based Cortex Data Lake for analysis.



Ex. 34, https://paloaltofirewalls.co.uk/cortex-xdr-managed-detection-and-response/.

146. The '903 Accused Products "monitors internal traffic as well as outbound traffic from clients and servers to the internet," including network devices that include a proxy, and build profiles from the logs based on "frequency of connections," test periods (e.g. 10 minutes or "10 KB or more were sent encoded in subdomain names during a 10-minute window") as well as the number of endpoints in your network that access certain domains "over time." Ex. 35 at 5,

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/stop-targeted-attacks-without-decrypting-traffic; Ex. 44 at 21, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference.pdf. The monitored network traffic includes requests for content from network hosts, which would cause the network host to transmit content. For example, a client system requesting content from a web site would cause the web site to transmit web content to the client.

147. The '903 Accused Products determines differences in transmission and receipt times in detecting attack tactics. For example, it detects the discovery tactic "by looking for symptoms in your internal network traffic such as changes in connectivity patterns that including increased rates of connections." In another, it detects whether an endpoint is controlled by a command and control server by looking "for anomalies in outbound connections" and "for unexplained changes in the periodicity of connections." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

148. The '903 Accused Products uses an analytics engine to correlate and compare data by examining logs and data from your sensors. The analytics engine retrieves logs from Cortex Data Lake to understand the normal behavior (creates a baseline) so that it can raise alerts when abnormal activity occurs. Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

149. The '903 Accused Products also uses Log Stitching and the Causality Analysis Engine to correlate and compare logs and event data to establish causality chains that identify the root cause, including identifying "a complete forensic timeline of events that helps you to

determine the scope and damage of an attack" and "the sequence of activity that led to the alert." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html; Ex. 45, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-pro-admin.pdf.

150. The '903 Accused Products analyze the data the NGFW collects and generate "an analytics alert when the analytics engine determines an anomaly…and use alerts to notify you of that abnormal behavior." The '903 Accused Products use the analytics engine to "examine traffic and data from a variety of sources such as network activity from firewall logs …to identify endpoints and users on your network." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

ıdpoint and net-
ex XDR can pin-
ımalware. It can
us sequences of
ɛ endpoint, such
ɔ shut down an
ication, suspi-
ations, registry
ɔre than a hundred other signs of malware and
ɛndpoint. With behavioral analytics, it can also
-based malware activity.

Focus on Network-Level Information, Not Application Contents

To detect attacks from unmanaged devices, Cortex XDR primarily inspects network metadata, such as traffic source, destination, domain, protocol, port number, and volume, which can be obtained from packet headers even when application-level content is encrypted.

Cortex XDR analyzes data Next-Generation Firewalls collect to track the normal behavior of users and devices, including the systems they access, the protocols they use, the amount of traffic they send and receive, and more. If Cortex XDR detects anomalous activity, it will generate an alert. Because it can detect attacks without inspecting application contents, application-level encryption does not affect detection (see figure 3).

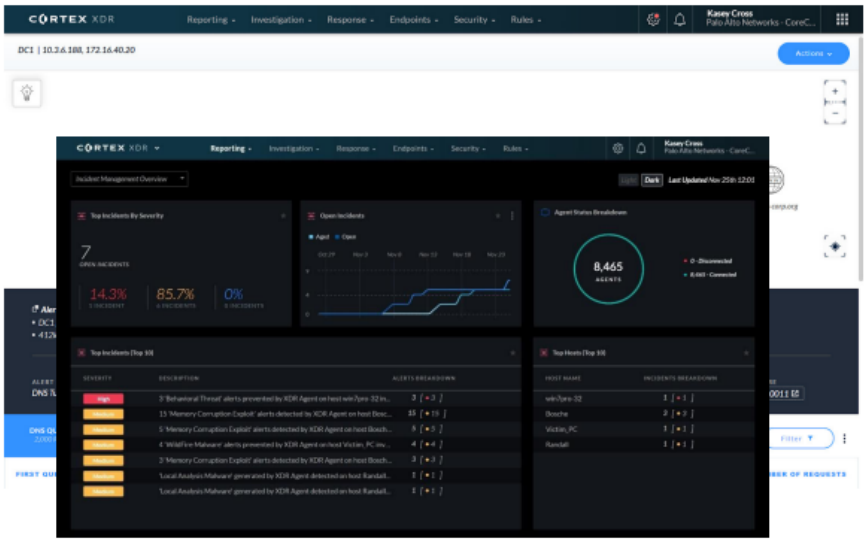


Figure 3: Cortex XDR detects network port scans even if individual requests are encrypted

Ex. 35 at 4,

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/stop-targeted-attacks-without-decrypting-traffic.

151. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

152. PAN has willfully infringed the '903 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '903 Patent

through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

153. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '903 Patent.

154. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

155. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '903 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '903 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '903 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

156. PAN's infringement of the '903 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

157. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

158. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SIXTH CAUSE OF ACTION
(Indirect Infringement of the '903 Patent)

159. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

160. PAN has induced and continues to induce infringement of one or more claims of the '903 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '903 Patent under 35 U.S.C. § 271(c).

161. PAN has induced infringement of the '903 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '903 Patent, including Claims 1-8 and 10-17.

162. PAN has knowingly and actively aided and abetted the direct infringement of the '903 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '903 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '903 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement, but is not limited to: advising third parties to use the '903 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a

mechanism through which third parties may infringe; by advertising and promoting the use of the '903 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '903 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

163. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '903 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '903 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

164. PAN contributorily infringes the '903 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '903 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '903 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be

used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '903 Patent, including Claims 1-8 and 10-17.

165. PAN has knowingly and actively contributed to the direct infringement of the '903 Patent by its manufacture, use, offer to sell, sale and importation of the '903 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '903 Patent as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

166. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

167. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '903 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '903 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '903 Patent.

168. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SEVENTH CAUSE OF ACTION
(Direct Infringement of the '573 Patent pursuant to 35 U.S.C. § 271(a))

169. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

170. PAN has infringed and continues to infringe a least Claims 1, 3-9, 11-17, and 19-24 of the '573 Patent.

171. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

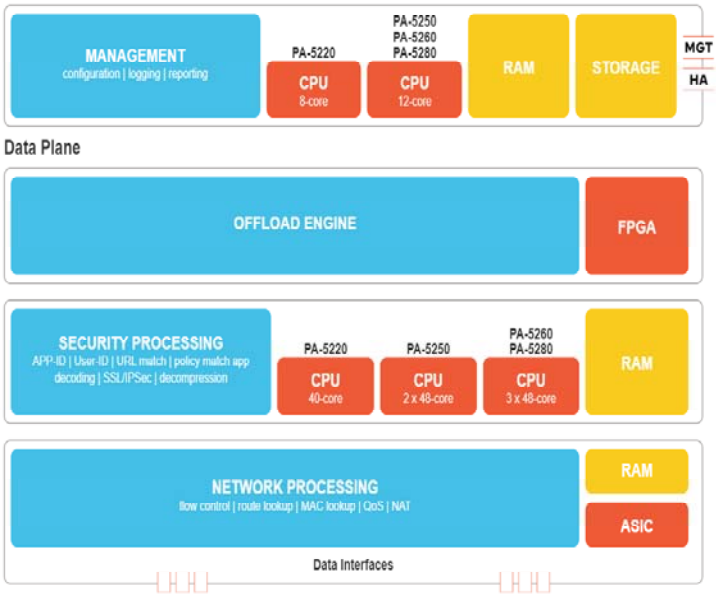
172. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

173. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '573 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Cortex, AutoFocus, and/or MineMeld (the "'573 Accused Products"). Combinations of the '573 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '573 Accused Products infringe under at least the following scenarios: (1) NGFW, (2) Cortex, and (3) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus or MineMeld. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits

from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

174. The '573 Accused Products embody the patented invention of the '573 Patent and infringe the '573 Patent because they identify a plurality of packets received by a network device from a host located in a first network; generate a first plurality of log entries corresponding to the plurality of packets received by the network device; identify a plurality of encrypted packets transmitted by the network device to a host located in a second network; generate a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device; correlate, based on the first plurality of log entries corresponding to the plurality of packets received by the network device and the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and responsive to the correlating of the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device: generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provision a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.

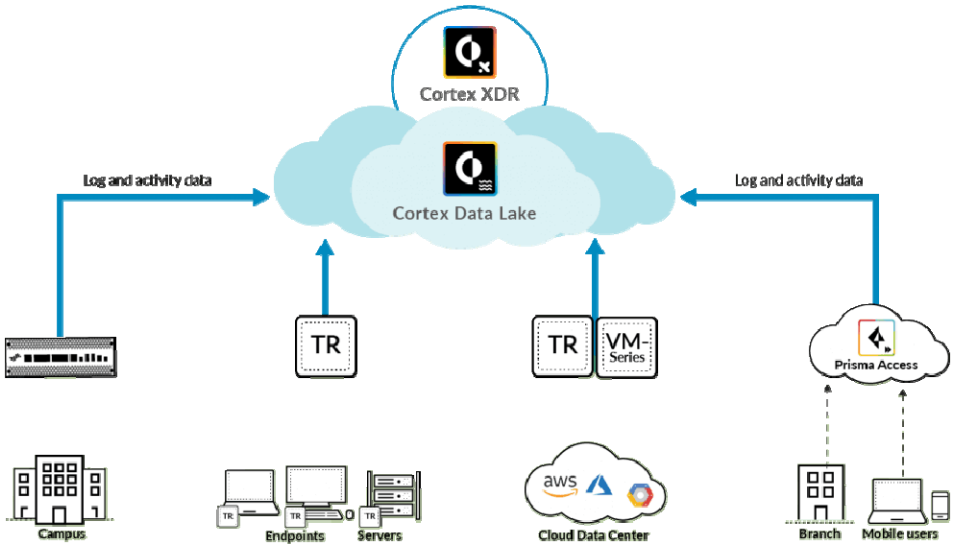
175. For example, as shown below, the '573 Accused Products include at least one processor and memory comprising instructions that, when executed by the at least one processor, cause a computing device to perform functionalities.



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

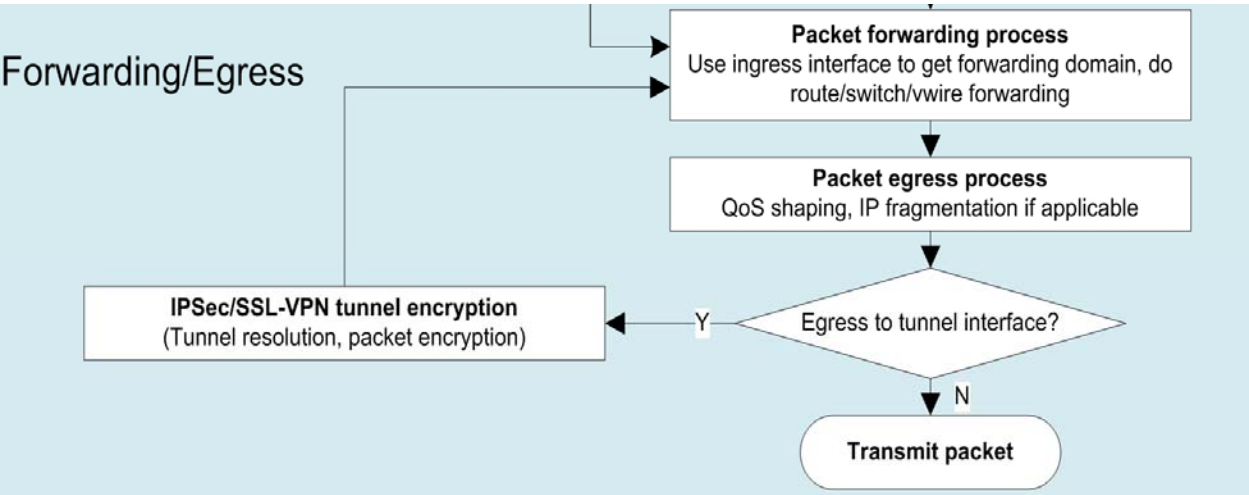
176. Additionally, Cortex XDR is run on servers with processors and memory and is used for Network Traffic Analysis to monitor internet traffic as well as internal, east-west communications between your users and servers to detect post-intrusion activity, such as lateral movement and exfiltration. Ex. 33, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf.

177. Further, NGFWs generate log data which are collected and stored in the cloud-based Cortex Data Lake for analysis as shown below:



Ex. 34, https://paloaltofirewalls.co.uk/cortex-xdr-managed-detection-and-response.

178. The '573 Accused Products also identify encrypted packets which are forwarded to a host located on a second network:



Ex. 37, https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.

179. The '573 Accused Products generate traffic logs for received and transmitted encrypted packets and have fields for the number of total packets (transmit and receive) for the session, the number of server-to-client packets for the session, the number of client-to-server

packets for the session, Tunnel ID, Tunnel Type (tunnel), SSL session is decrypted (SSL Proxy) or payload of the outer tunnel is being inspected. Ex. 38, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf.

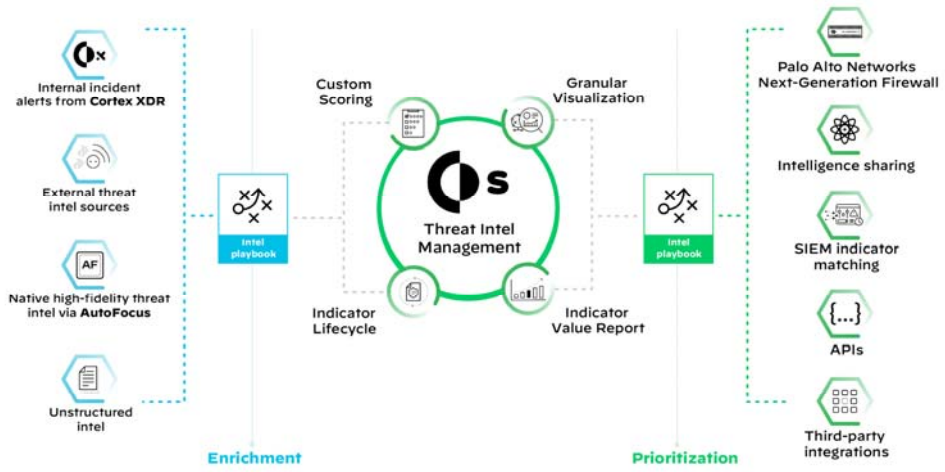
180. The Automated Correlation Engine uses the logs on the firewall to detect actionable events on your network and correlates a series of related threat events that indicate a likely compromised host or other high level conclusion. Ex. 39, https://www.birdrockusa.com/blog/bird-rock-systems-technology-blog/2015/7/10/palo-alto-firewall-pan-os-70-is-here.html.

181. Further, Cortex XDR correlates log entries of packets received and transmitted by monitoring internal traffic as well as outbound traffic from clients and servers to the internet and analyzing protocol-level metadata traffic logs that are collected by NGFWs, and building a profile based on source and destination traffic. Cortex XDR's log correlation, includes logs for encrypted packets by using the analytics engine to examine traffic and data from a variety of sources such as network activity from firewall logs and VPN logs. Ex. 35, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/stop-targeted-attacks-without-decrypting-traffic; Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html. For example, Cortex XDR may correlate encrypted packets transmitted by a network device with packet received by the network device to identify a suspicious host in a network.

182. Based on the correlation, Cortex XDR generate rules used by the NGFW using sensor integration to allow new data sources to continually add to the NGFW, which are used

to identify suspicious activity such as a suspicious host in a network transmitting malicious packets. Ex. 23, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

183. Further, Cortex XSOAR's Threat Intel Management is used to create block/accept policies (Source, Destination, Port), for IP addresses and domains in the NGFW.



Ex. 28, https://www.paloaltonetworks.com/cortex/threat-intel-management.

184. Additionally, AutoFocus uses miners to dynamically send indicators from AutoFocus to an external dynamic list on the NGFW to enforce security policy on the firewall. Ex. 40, https://docs.paloaltonetworks.com/autofocus/autofocus-admin/get-started-with-autofocus/use-autofocus-with-the-palo-alto-networks-firewall.

185. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

186. PAN has willfully infringed the '573 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '573 Patent

through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

187. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '573 Patent.

188. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

189. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '573 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '573 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '573 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

190. PAN's infringement of the '573 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

191. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

192. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

EIGHTH CAUSE OF ACTION
(Indirect Infringement of the '573 Patent)

193. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

194. PAN has induced and continues to induce infringement of one or more claims of the '573 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '573 Patent under 35 U.S.C. § 271(c).

195. PAN has induced infringement of the '573 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '573 Patent, including Claims 1, 3-9, 11-17, and 19-24.

196. PAN has knowingly and actively aided and abetted the direct infringement of the '573 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '573 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '573 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '573 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a

mechanism through which third parties may infringe; by advertising and promoting the use of the '573 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '573 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

197. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '573 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '573 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

198. PAN contributorily infringes the '573 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '573 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '573 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be

used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '573 Patent, including Claims 1, 3-9, 11-17, and 19-24.

199. PAN has knowingly and actively contributed to the direct infringement of the '573 Patent by its manufacture, use, offer to sell, sale and importation of the '573 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '573 Patent as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

200. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

201. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '573 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '573 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '573 Patent.

202. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

NINTH CAUSE OF ACTION
(Direct Infringement of the '437 Patent pursuant to 35 U.S.C. § 271(a))

203. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

204. PAN has infringed and continues to infringe a least Claims 1, 3-8, 10-15, and 17-20 of the '437 Patent.

205. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

206. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

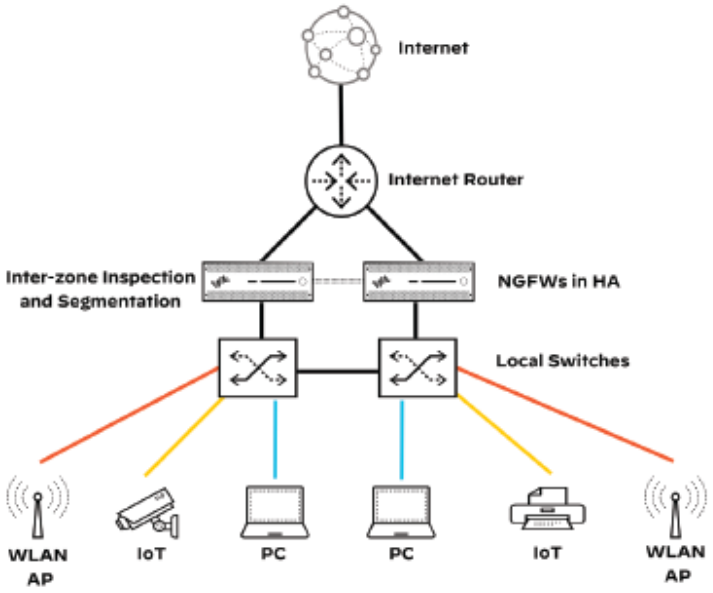
207. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '437 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Cortex, AutoFocus, and/or MineMeld (the "'437 Accused Products"). Combinations of the '437 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '437 Accused Products infringe under at least the following scenarios: (1) NGFW, (2) Cortex, and (3) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus or MineMeld. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits

from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

208. The '437 Accused Products embody the patented invention of the '437 Patent and infringe the '437 Patent because they include at least one processor; and memory storing instructions that when executed by the at least one processor cause the system to: provision a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, with one or more packet filtering rules to be applied to all network traffic traversing the boundary, wherein each packet filtering rule comprises at least one packet matching criterion associated with malicious network traffic and a corresponding packet transformation function; and configure the packet security gateway to: receive, via a communication interface that does not have a network-layer address, network traffic traversing the boundary via the packet security gateway, wherein the network traffic comprises received packets and is associated with each host of a plurality of hosts located in the network protected by the packet security gateway, and wherein the received packets comprise: first packets traversing the boundary, via the packet security gateway, that originate from outside the network protected by the packet security gateway and are destined for the plurality of hosts; and second packets traversing the boundary, via the packet security gateway, that originate from the plurality of hosts located in the network and are destined for devices in the one or more networks other than the network protected by the packet security gateway; responsive to a determination by the packet security gateway that a portion of the received packets corresponds to at least one packet matching criterion specified

by the one or more packet filtering rules, drop the portion of the received packets; and modify a switching matrix of a local area network (LAN) switch associated with the packet security gateway such that the LAN switch is configured to drop the portion of the received packets responsive to the determination by the packet security gateway.

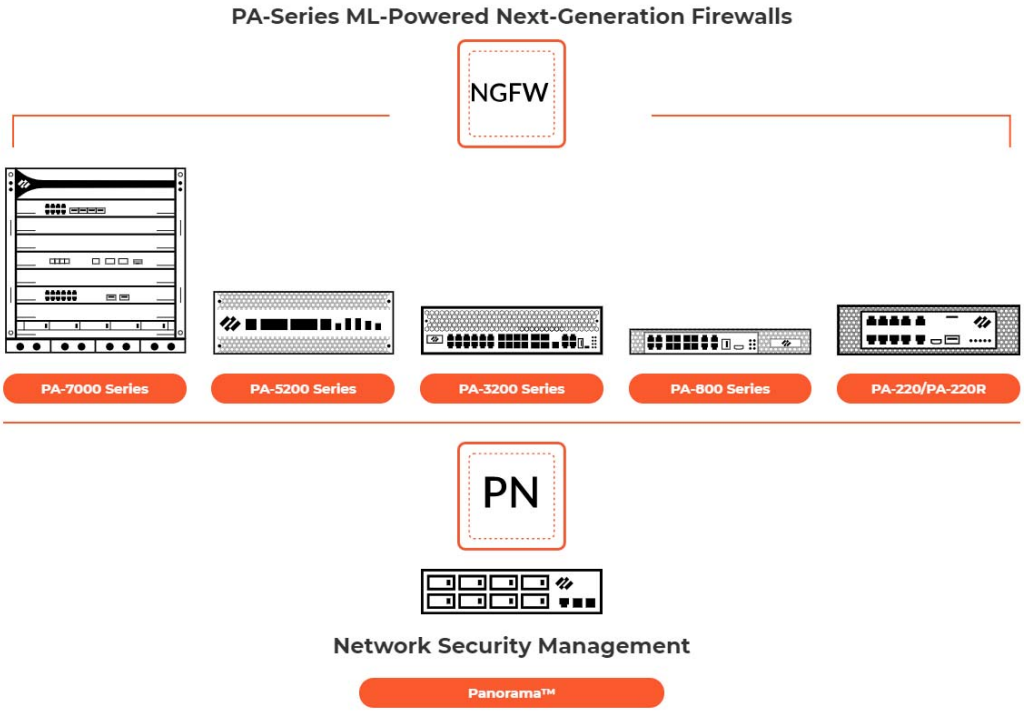
209. The '437 Accused Products are packet security gateways that protect organizations and data centers at the network perimeter. The '437 Accused Products run on computer systems with a processor, main memory, and RAM. The memory stores the instructions that are executed by the processor.



Ex. 29 at 27-28, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

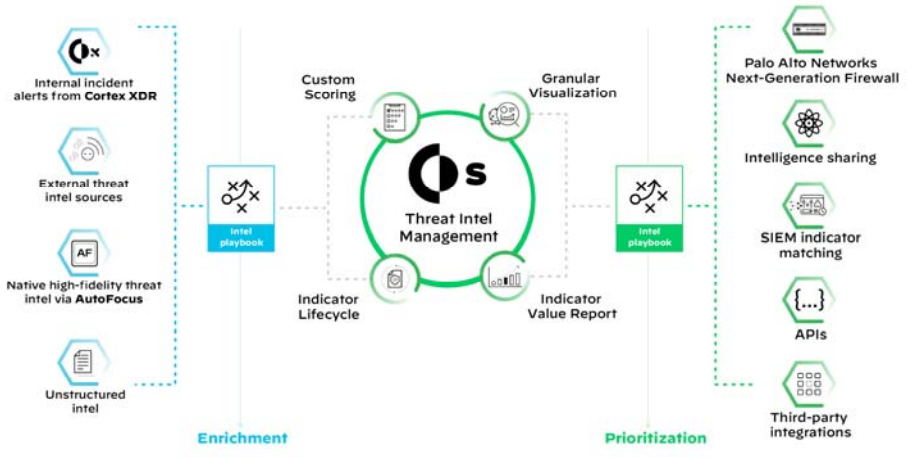
210. For example, Panorama provisions one or more of the NGFW with packet filtering rules applied to all traffic traversing a network boundary. The packet filtering rules include packet matching criterion which are used to filter network packets that match the criterion according to a corresponding packet transformation function, such as deny or allow. The NGFW(s) deployed in a network collectively provide an interface across a boundary of the

network and implement a "zero trust" system where all traffic must be validated and may block or allow traffic based on rules. Additionally, the '437 Accused Products, integrate logs, malware analysis reports, and visibility into malicious events, including by using PAN-OS, Panorama network security management, AutoFocus contextual threat intelligence service, Cortex XSOAR, and Cortex XDR. As an example, Panorama includes subscription services such as AutoFocus threat feeds, which include malicious traffic information such as IP addresses, domains, URLs, and hash indicators and is continually updated and form the packet filtering rules. Additionally, AutoFocus includes a threat intelligence analysis database (including information, such as malicious traffic information, from multiple sources like WildFire, Unit 42, and third party feeds) that create rules (e.g. threat feed or threat indicators) which are provisioned to packet-filtering devices (e.g. NGFW) using MineMeld and form the packet filtering rules. Panorama and NGFW also includes independent network-threat-intelligence providers (supported threat feed sources).



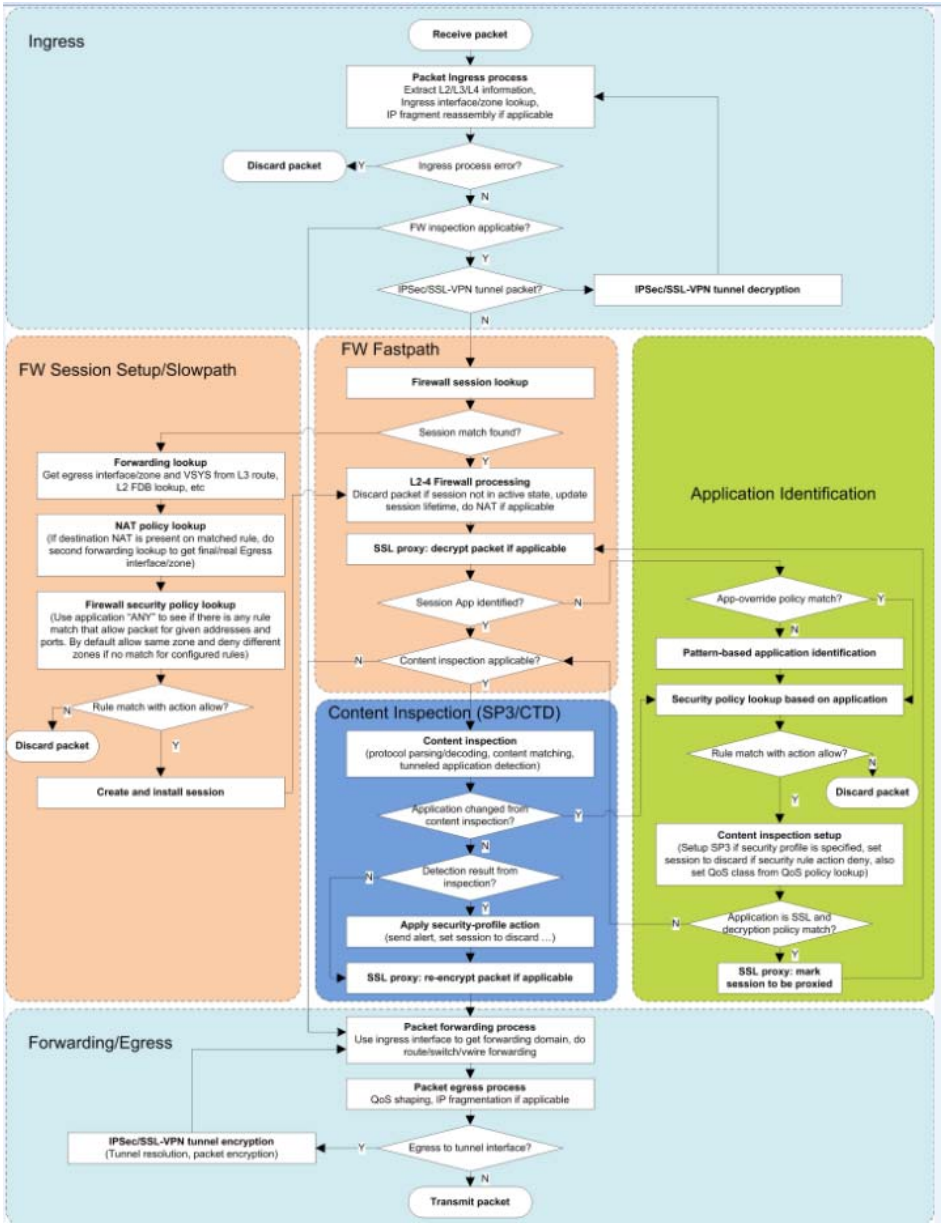
Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

211. Additionally, the NGFW is provisions with dynamic security policies with packet filtering rules, such as create block/accept policies (Source, Destination, Port), for IP addresses and domains in the PAN-OS firewalls, from Cortex, which is a security policy management server. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers.



Ex. 28, https://www.paloaltonetworks.com/cortex/threat-intel-management.

212. Further, NGFW receives network traffic via a Layer 2 interface, which does not have a network layer address. The NGFW receives all traffic traversing the network and applies a single-pass architecture, which processes each packet, including for policy lookup, decoding, threat detection, content checking, application checking, and networking. The NGFW will parse each packet's layer 2 header information. Additionally, the NGFW inspects all incoming and outgoing packets, allowing Panorama to aggregates logs from all managed firewalls and provides visibility across all the traffic on the network.



Ex. 37,

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.

213. Thus, NGFW automatically modifies the switching matrix of the LAN switches to block (drop) or allow network traffic depending on the policy or rules, or criterion in the policy or rules, because it oversees all traffic and executes all management functions, including directing traffic to the appropriate data processing. Additionally, the NGFW operates with a

Firewall Switch Management Card that modify the switching matrix of the LAN switch to drop traffic based on packet filtering rules, or a determination by the NGFW that network traffic matches criterion on the packet filtering rules.

214. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

215. PAN has willfully infringed the '437 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '437 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

216. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '437 Patent.

217. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

218. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '437 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '437 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '437 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

219. PAN's infringement of the '437 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

220. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

221. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TENTH CAUSE OF ACTION
(Indirect Infringement of the '437 Patent)

222. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

223. PAN has induced and continues to induce infringement of one or more claims of the '437 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '437 Patent under 35 U.S.C. § 271(c).

224. PAN has induced infringement of the '437 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '437 Patent, including Claims 1, 3-8, 10-15, and 17-20.

225. PAN has knowingly and actively aided and abetted the direct infringement of the '437 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '437 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '437 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '437 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '437 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '437 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

226. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '437 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '437 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers,

vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

227. PAN contributorily infringes the '437 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '437 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '437 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '437 Patent, including Claims 1, 3-8, 10-15, and 17-20.

228. PAN has knowingly and actively contributed to the direct infringement of the '437 Patent by its manufacture, use, offer to sell, sale and importation the '437 Accused Products together with its manufacturers customers, purchasers, users, developers, and/or vendors to meet the elements of the '437 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

229. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

230. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '437 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '437 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '437 Patent.

231. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

ELEVENTH CAUSE OF ACTION
(Direct Infringement of the '266 Patent pursuant to 35 U.S.C. § 271(a))

232. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

233. PAN has infringed and continues to infringe a least Claims 1-4, 7-11, 14-17, 20-24, and 27 of the '266 Patent.

234. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

235. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

236. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '266 Patent, these products, services, and technologies including, but not limited to the

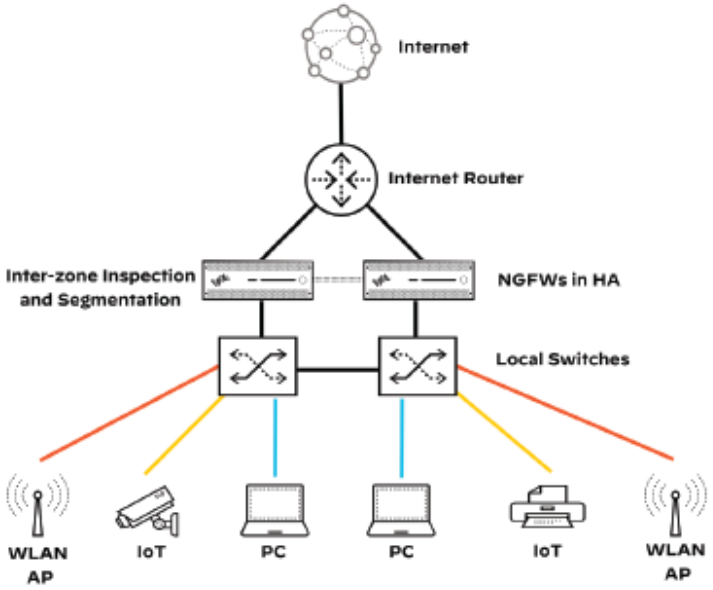
marketing names: NGFW, Cortex, AutoFocus, and/or MineMeld (the "'266 Accused Products"). Combinations of the '266 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '266 Accused Products infringe under at least the following scenarios: (1) NGFW and (2) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus or MineMeld. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

237. The '266 Accused Products embody the patented invention of the '266 Patent and infringe the '266 Patent because they are a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising: one or more processors; and memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to: receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein: each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or

more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets; receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

238. The ‘266 Accused Products are packet security gateways that protect organizations and data centers at the network perimeter. The ‘266 Accused Products run on

computer systems with a processor, main memory, and RAM. The memory stores the instructions that are executed by the processor.

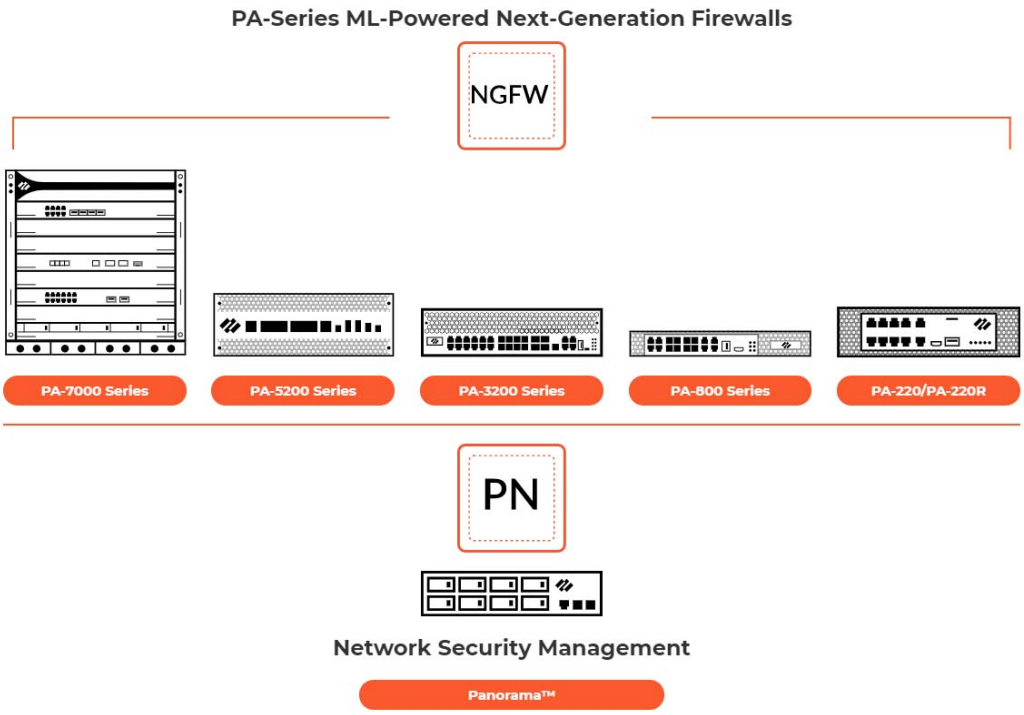


Ex. 29 at 27-28, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

239. For example, Panorama, which is a security policy management server, provisions one or more of the NGFW with packet filtering rules applied to all traffic traversing a network boundary. The NGFW(s) deployed in a network collectively provide an interface across a boundary of the network and implement a "zero trust" system were all traffic must be validated and may block or allow traffic based on rules, such as packet filtering rules, including a "first set of packet filtering rules" and an updated "second set of packet filtering rules." The packet filtering rules include packet matching criterion which are used to filter network packets that match the criterion according to a corresponding packet transformation function, such as deny or allow. Additionally, the '266 Accused Products, integrate logs, malware analysis reports, and visibility into malicious events, including by using PAN-OS, Panorama network security management, AutoFocus contextual threat intelligence service, Cortex XSOAR, and

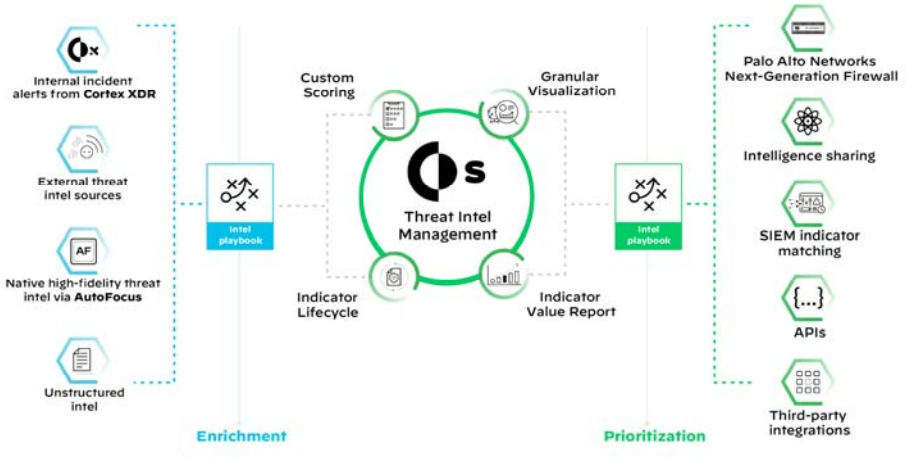
Cortex XDR. As an example, Panorama includes AutoFocus threat feeds, which include malicious traffic information such as IP addresses, domains, URLs, and hash indicators and is continually updated and form the packet filtering rules, including the "updated second set of packet filtering rules." Additionally, AutoFocus includes a threat intelligence analysis database (including information, such as malicious traffic information, from multiple sources like WildFire, Unit 42, and third party feeds, which track malicious host activity from network hosts) that create rules (e.g. threat feed or threat indicators) which are provisioned to packet-filtering devices (e.g. NGFW) using MineMeld and form the packet filtering rules. Panorama and NGFW also includes independent network-threat-intelligence providers (supported threat feed sources).

240. As an example, Panorama includes subscription services such as AutoFocus threat feeds, which include malicious traffic information such as IP addresses, domains, URLs, and hash indicators and is continually updated and form the packet filtering rules. Additionally, AutoFocus includes a threat intelligence analysis database (including information, such as malicious traffic information, from multiple sources like WildFire, Unit 42, and third party feeds) that create rules (e.g. threat feed or threat indicators) which are provisioned to packet-filtering devices (e.g. NGFW) using MineMeld and form the packet filtering rules. Panorama and NGFW also includes independent network-threat-intelligence providers (supported threat feed sources).



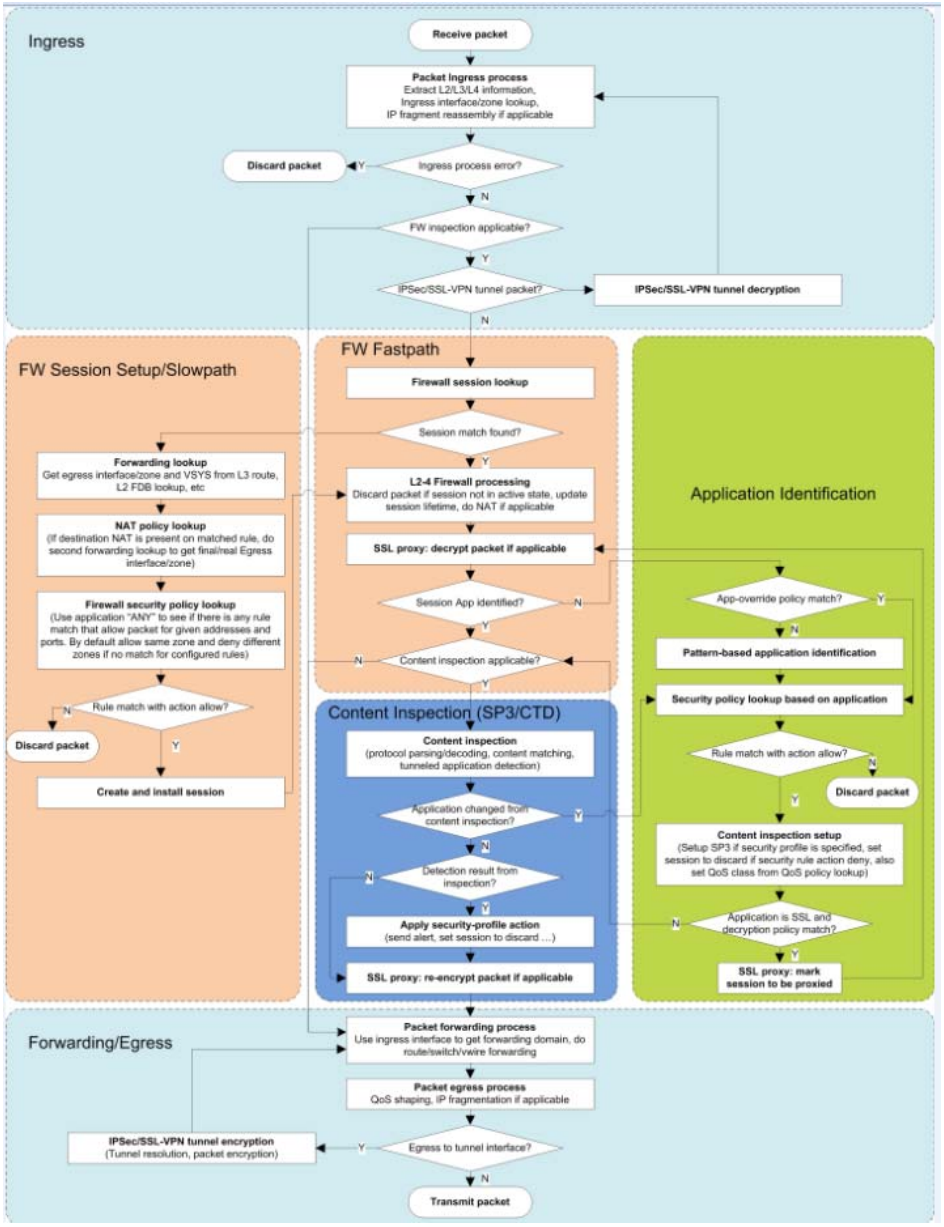
Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

241. Additionally, the NGFW is provisioned with dynamic security policies with packet filtering rules, such as create block/accept policies (Source, Destination, Port), for IP addresses and domains in the PAN-OS firewalls, from Cortex, which is a security policy management server. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers.



Ex. 28, https://www.paloaltonetworks.com/cortex/threat-intel-management.

242. Further, the '266 Accused Products receive all traffic traversing the network and applies a single-pass architecture, which processes each packet, including for policy lookup, decoding, threat detection, content checking, application checking, and networking. For example, the NGFW will inspect all incoming and outgoing packets, allowing Panorama to aggregates logs from all managed firewalls and provides visibility across all the traffic on the network.



Ex. 37,

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.

243. The '266 Accused Products are automatically updated with new rules that are applied to subsequent packets. For example, Panorama will update the NGFW as new threat information is made available from the utilized threat services, which allows new and updated rules to be applied to subsequent packets, such as create block/accept policies.

244. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

245. PAN has willfully infringed the '266 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '266 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

246. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '266 Patent.

247. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

248. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '266 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '266 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '266 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

249. PAN's infringement of the '266 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

250. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

251. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWELFTH CAUSE OF ACTION
(Indirect Infringement of the '266 Patent)

252. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

253. PAN has induced and continues to induce infringement of one or more claims of the '266 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '266 Patent under 35 U.S.C. § 271(c).

254. PAN has induced infringement of the '266 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '266 Patent, including Claims 1-4, 7-11, 14-17, 20-24, and 27.

255. PAN has knowingly and actively aided and abetted the direct infringement of the '266 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '266 Patent with the Accused

Products. Such use is consistent with how the products are described to directly infringe the '266 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '266 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '266 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '266 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

256. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '266 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '266 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

257. PAN contributorily infringes the '266 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '266 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '266 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it was contributing to the infringement of one or more claims of the '266 Patent, including Claims 1-4, 7-11, 14-17, 20-24, and 27.

258. PAN has knowingly and actively contributed to the direct infringement of the '266 Patent by its manufacture, use, offer to sell, sale and importation of the '266 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '266 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

259. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

260. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '266 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '266 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '266 Patent.

261. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

THIRTEENTH CAUSE OF ACTION
(Direct Infringement of the '343 Patent pursuant to 35 U.S.C. § 271(a))

262. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

263. PAN has infringed and continues to infringe a least Claims 1-3, 5, 7-10, 12, 14-17, and 20 of the '343 Patent.

264. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

265. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

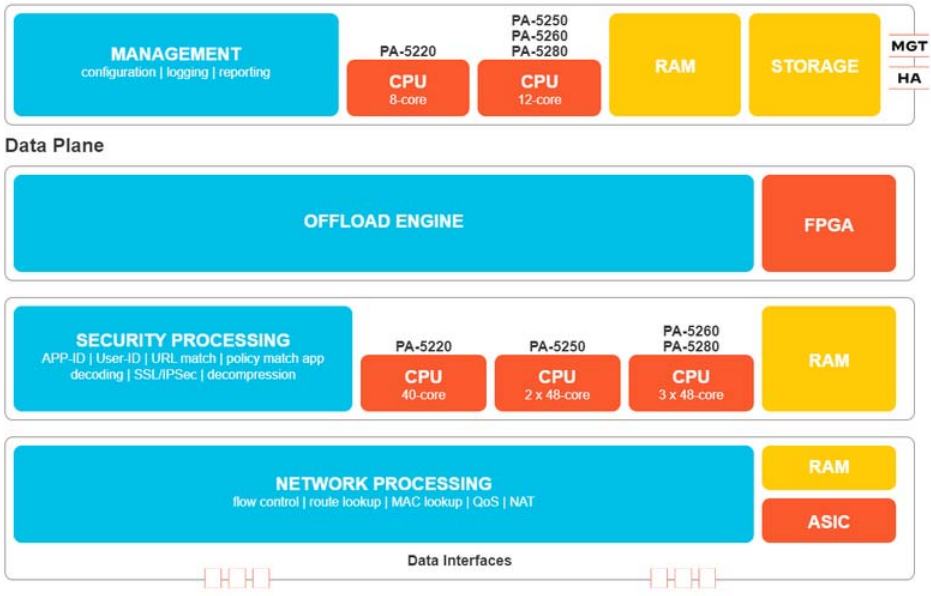
266. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '343 Patent, these products, services, and technologies including, but not limited to the

marketing names: NGFW, Panorama, Enterprise DLP service, and/or DNS Security Service (the "'343 Accused Products"). Combinations of the '343 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '343 Accused Products infringe under at least the following scenarios: (1) NGFW and (2) NGFW and Panorama, with any of the scenarios alone or in combination with Enterprise DLP service or DNS Security Service. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

267. The '343 Accused Products embody the patented invention of the '343 Patent and infringe the '343 Patent because they include at least one processor; and memory comprising instructions that, when executed by the one or more processors, cause the apparatus to: receive a plurality of packets; determine, based on a packet header field value, whether the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules; responsive to a determination that a packet header field value of a first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, apply, to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule; determine, based on an application header field value, a second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and responsive to determining the

second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, apply, to each packet in the second portion of packets, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

268. As shown below, the '343 Accused Products include system components that include one or more processors and memory including instructions. For instance, the NGFW PA-series runs an operating system PAN-OS stored in the memory and executed by the processors. The functionality of the PAN-OS provides a common operating system that "runs on all Palo Alto Networks ML-powered NGFWs."

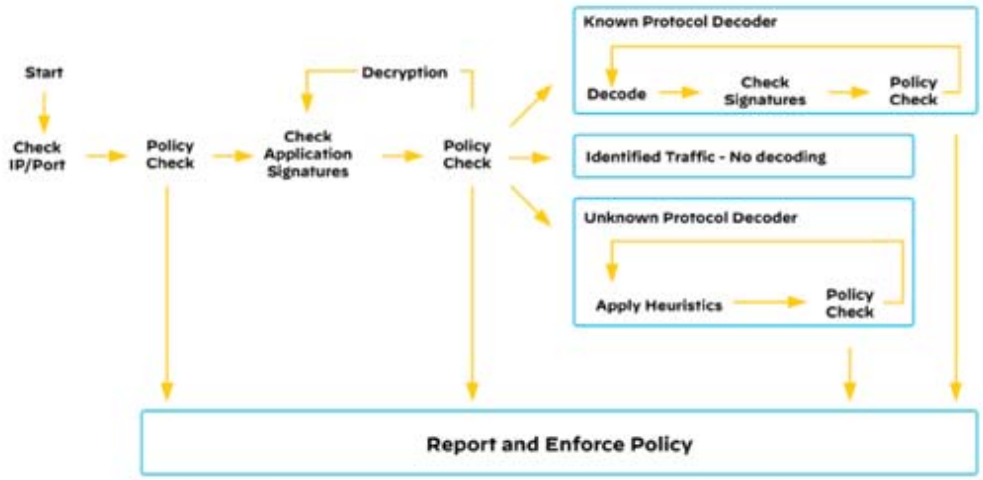


Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures; Ex. 16, https://docs.paloaltonetworks.com/pan-os.html.

269. Further, the '343 Accused Products incorporate App-ID technology, which is a traffic classification engine that "classifies all network traffic across all ports, enabling

administrators to create logical application-based security policies," based on header field values of packets and application packets.

Figure 6 App-ID policy enforcement



App-ID classifies all network traffic across all ports, enabling administrators to create logical application-based security policies. App-ID uses multiple identification techniques to identify applications passing through the network. This helps with threats such as lateral movement when adversaries try to mask applications' port numbers in order to evade detection. App-ID combined with User-ID gives you better visibility into what is traversing your network. You can treat unknown traffic as a separate category and handle it based on your organization's risk profile.

Ex. 29 at 20, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

270. Further, the '343 Accused Products use security policies and packet filtering rules for preventing data exfiltration by identifying and determining, according to the security policies and packet filtering rules, packets that are bound for an untrusted destination zone and that are identified as traffic for data-transfer-related protocols and applications. The packet filtering rules include criterion which are used to filter network packets that match the criterion according to a corresponding packet transformation function, such as deny or allow.

		Source				Destination				
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Block peer to peer	none	trustL3	any	any	any	untrustL3	any	bittorrent kazaa	any	
Block file sharing	none	trustL3	any	any	any	untrustL3	any	aim-file-transfer filesonic msn-file-transfer rapidshare	any	
Allow Other Web	none	trustL3	any	any	any	untrustL3	any	any	service-http service-https	
Cleanup Rule	none	any	any	any	any	any	any	any	any	

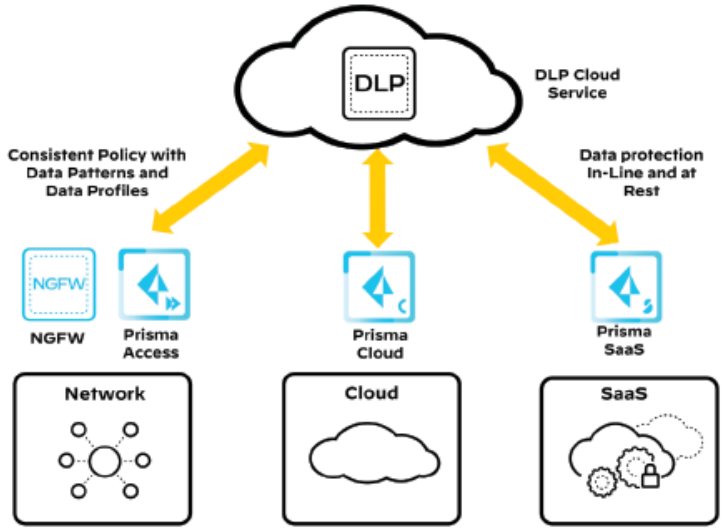
Ex. 41 at 9-10, https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000U0roAAC&field=Attachment_1__Body__s.

271. Further, the '343 Accused Products incorporate Enterprise DLP technology, a cloud-based subscription service that is designed to protect against unauthorized access, misuse, extraction, and sharing of sensitive information and effectively filter network traffic to block or generate an alert before sensitive information leaves the network. The Enterprise DLP technology enables the NGFW to detect network exfiltration in network traffic using security policies.

Enterprise Data Loss Prevention Features

New Enterprise DLP Feature	Description
Enterprise Data Loss Prevention (DLP)	To protect against unauthorized access, misuse, extraction, and sharing of sensitive information, you need to effectively filter network traffic to block or generate an alert before sensitive information leaves the network. Enterprise Data Loss Prevention (DLP) provides a single engine for accurate detection and consistent policy enforcement for sensitive data at rest and in motion. Panorama and managed firewalls running PAN-OS 10.0.2 and later releases support Enterprise DLP.

Ex. 42 at 7, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-release-notes/pan-os-release-notes.pdf.



Ex. 29 at 39-41, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

272. Moreover, the '343 Accused Products set up cloud-based DNS Security Service to access an infinitely scalable DNS signature and protection sources to defend against malicious domains. The DNS security service operates real-time DNS request analysis using predictive analytics and machine learning on multiple DNS sources. Further, DNS Security Service to detect Command and Control Domains (C2) which include URLs (e.g. **HTTP**) and domains used by malware and/or compromised systems to communicate with an attacker's remote server to exfiltrate data. As shown below, the DGA detection prevents data exfiltration by identifying and blocking a domain generated in large amount by a machine. The DNS tunnel detection prevents data exfiltration hidden in the DNS queries and responds through policy rules.

- **Command and Control Domains**—C2 include URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data (this includes DNS tunneling detection and DGA detection).
  - **DNS Tunnel Detection**—DNS tunneling can be used by attackers to encode data of non-DNS programs and protocols within DNS queries and responses. This provides attackers with an open back channel with which they can transfer files or remotely access the system. DNS tunnel detection uses machine learning to analyze the behavioral qualities of DNS queries, including n-gram frequency analysis of domains, entropy, query rate, and patterns to determine if the query is consistent with a DNS tunneling-based attack. Combined with the firewall's automated policy actions, this allows you to quickly detect C2 or data theft hidden in DNS tunnels and to automatically block it, based on your defined policy rules.
  - **DGA Detection**—Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values. While most domains generated by a DGA do not resolve as a valid domain, they must all be identified to fully defend against a given threat. DGA analysis determines whether a domain is likely to have been generated by a machine, rather than a person, by reverse-engineering and analyzing other frequently used techniques found in DGAs. Palo Alto Networks then uses these characteristics to identify and block previously unknown DGA-based threats in real-time.

Ex. 38 at 741, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf.

273. The Accused Products will detect the anomalies in the HTTP requests to malicious hosts that intend to exfiltrate data through DNS traffic. Once the malicious hosts are identified, the Accused Products conduct verification through data exchanges between the requestors and the malicious hosts. As shown below, the Accused Products can perform transformations on packets and will either block all unknown applications and traffic using the security policy or direct exfiltration to a "sinkhole," a designated IP tunnel to steer away from malicious domains.

- ☐ Block all unknown applications and traffic using the Security policy. Typically, the only applications classified as unknown traffic are internal or custom applications on your network and potential threats. Unknown traffic can be either non-compliant applications or protocols that are anomalous or abnormal or it can be known applications that are using non-standard ports, both of which should be blocked. See Manage Custom or Unknown Applications.

Ex. 38 at 728, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf.

Palo Alto Networks customers are protected in the following ways:

- All RDAT samples have malicious verdicts in WildFire and have protections in place through Cortex XDR.
- DNS tunneling protocols used for C2 communications are blocked via DNS Security.
- All C2 domains are classified as Command-and-Control for URL Filtering.
- AutoFocus customers can monitor activity via the rdat_backdoor tag.

Ex. 43 at 18, https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/.

274. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

275. PAN has willfully infringed the '343 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '343 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

276. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '343 Patent.

277. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

278. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '343 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '343 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '343 Patent, justifying an award to

Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

279. PAN's infringement of the '343 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

280. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

281. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FOURTEENTH CAUSE OF ACTION
(Indirect Infringement of the '343 Patent)

282. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

283. PAN has induced and continues to induce infringement of one or more claims of the '343 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '343 Patent under 35 U.S.C. § 271(c).

284. PAN has induced infringement of the '343 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is

inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '343 Patent, including Claims 1-3, 5, 7-10, 12, 14-17, and 20.

285. PAN has knowingly and actively aided and abetted the direct infringement of the '343 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '343 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '343 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '343 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '343 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '343 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

286. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '343 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the

operation of the '343 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

287. PAN contributorily infringes the '343 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '343 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '343 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '343 Patent, including Claims 1-3, 5, 7-10, 12, 14-17, and 20.

288. PAN has knowingly and actively contributed to the direct infringement of the '343 Patent by its manufacture, use, offer to sell, sale and importation of the '343 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '343 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and

methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

289. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

290. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '343 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '343 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '343 Patent.

291. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FIFTEENTH CAUSE OF ACTION
(Direct Infringement of the '380 Patent pursuant to 35 U.S.C. § 271(a))

292. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

293. PAN has infringed and continues to infringe a least Claims 1, 6-8, 10-13, 16-19, 21-22, and 25-27 of the '380 Patent.

294. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

295. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

296. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '380 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Panorama, Enterprise DLP, and/or DNS Security Service (the "'380 Accused Products"). Combinations of the '380 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '380 Accused Products infringe under at least the following scenarios: (1) NGFW and (2) NGFW and Panorama, with any of the scenarios alone or in combination with Enterprise DLP service or DNS Security Service. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

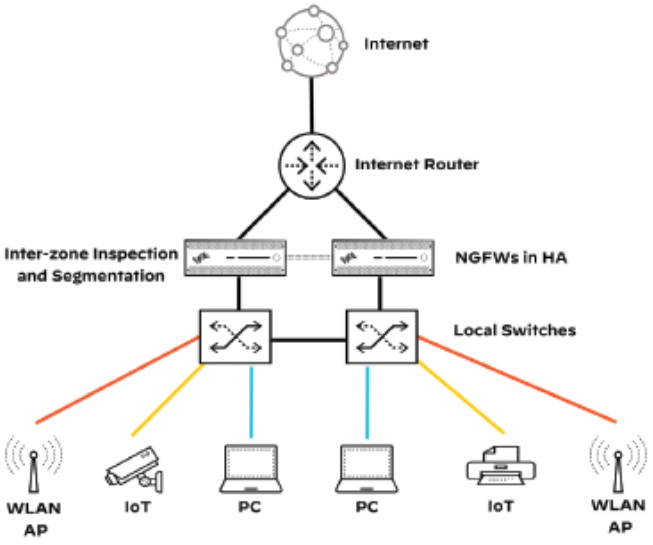
297. The '380 Accused Products embody the patented invention of the '380 Patent and infringe the '380 Patent because they include a packet security gateway that interfaces at a boundary of a protected network, and which includes one or more processors; and memory comprising instructions that, when executed by the one or more processors, cause the packet security gateway to: receive a plurality of outbound in-transit packets departing the protected network, wherein the plurality of outbound in-transit packets comprises first packets destined for a first destination; determine, based on one or more packet-filtering rules, that the first destination comprises a destination outside of the protected network; identify, based on a determination that the first destination comprises a destination outside of the protected

network, at least one application packet contained in the first packets; determine that the identified at least one application packet is associated with a data transfer protocol associated with the one or more packet-filtering rules; identify a data transfer request field within a header region of the identified at least one application packet; determine whether a value of the identified data transfer request field indicates that the data transfer protocol comprises one or more network exfiltration methods associated with the one or more packet-filtering rules; and apply one or more operators, specified by the one or more packet-filtering rules and based on a determination that the identified data transfer request field indicates one or more network exfiltration methods, to the first packets, wherein applying the one or more operators causes the first packets to be dropped.

298. The ’380 Accused Products include a packet security gateway that interfaces at a boundary of a protected network, as shown below.

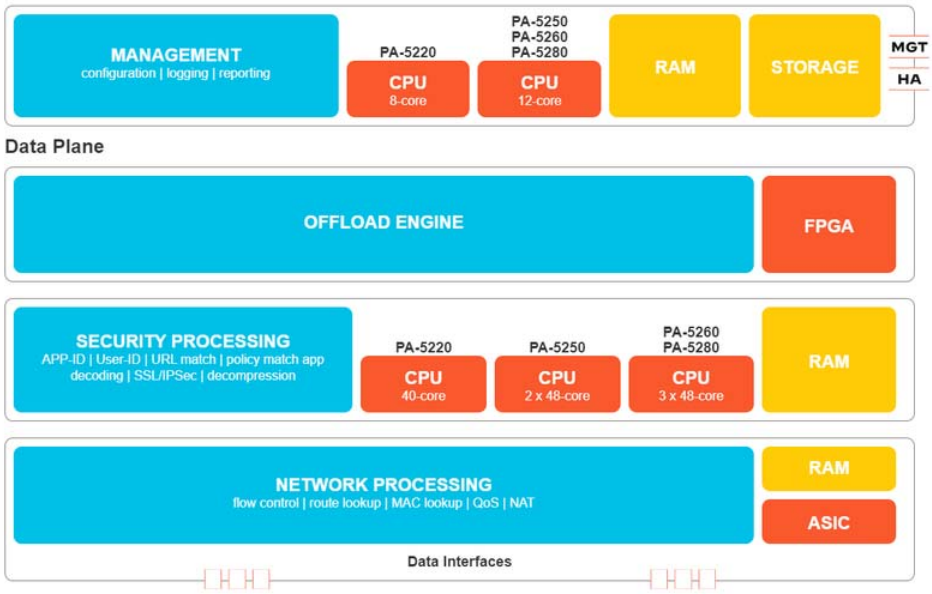
Deployment

At the branch or any remote site, you typically deploy a NGFW between the internet edge router and the local, Layer 2, switched network. The NGFW becomes the termination and routing point for virtual local area network (VLAN) connections. You can deploy NGFWs in high-availability (HA) mode, ensuring a firewall is always available and reducing operational downtime. HA deployment options include active-active and active-standby, where active-standby is the most common option. By using zones, you segment devices based on their type, such as separating IoT devices and user PCs.



Ex. 29 at 27-28, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

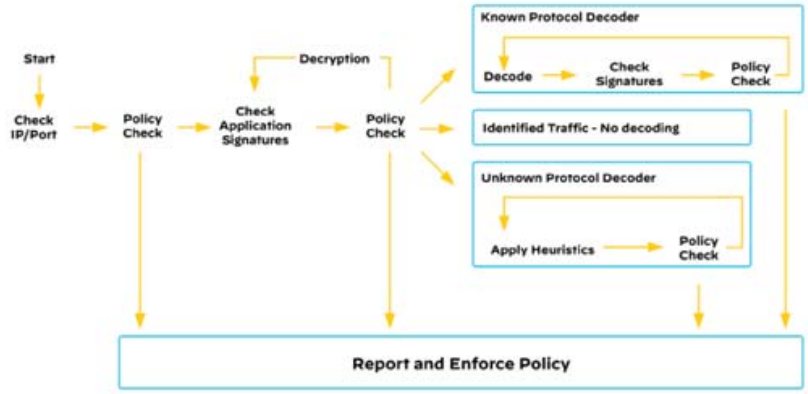
299. The '380 Accused Products include system components that include one or more processors and memory including instructions. For instance, and as shown below, the NGFW PA-series runs an operating system PAN-OS stored in the memory and executed by the processors.



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

300. Further, the '380 Accused Products incorporate App-ID technology, which is a traffic classification engine that "classifies all network traffic across all ports, enabling administrators to create logical application-based security policies."

Figure 6 App-ID policy enforcement



App-ID classifies all network traffic across all ports, enabling administrators to create logical application-based security policies. App-ID uses multiple identification techniques to identify applications passing through the network. This helps with threats such as lateral movement when adversaries try to mask applications' port numbers in order to evade detection. App-ID combined with User-ID gives you better visibility into what is traversing your network. You can treat unknown traffic as a separate category and handle it based on your organization's risk profile.

Ex. 29 at 20, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

301. Further, the '380 Accused Products use security policies and packet filtering rules for preventing data exfiltration by identifying and determining, according to the security policies and packet filtering rules, packets that are bound for an untrusted destination zone and that are identified as traffic for data-transfer-related protocols and applications. The packets include application packets which are associated with data transfer protocols, such as FTP, associated with the packet filtering rules.

		Source				Destination				
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Block peer to peer	none	trustL3	any	any	any	untrustL3	any	bittorrent kazaa	any	
Block file sharing	none	trustL3	any	any	any	untrustL3	any	aim-file-transfer filesonic msn-file-transfer rapidshare	any	
Allow Other Web	none	trustL3	any	any	any	untrustL3	any	any	service-http service-https	
Cleanup Rule	none	any	any	any	any	any	any	any	any	

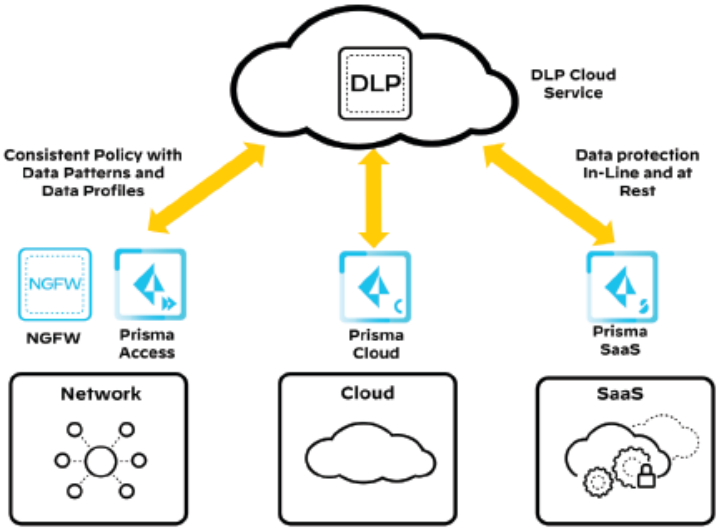
Ex. 41 at 9-10, https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000U0roAAC&field=Attachment_1__Body__s.

302. Additionally, the '380 Accused Products incorporate Enterprise DLP technology, a cloud-based subscription service that is designed to "protect against unauthorized access, misuse, extraction, and sharing of sensitive information" and "effectively filter network traffic to block or generate an alert before sensitive information leaves the network." The Enterprise DLP technology enables the NGFW to detect network exfiltration methods in network traffic using security policies and packet filtering rules, including analyzing data transfer request fields in application packet headers.

Enterprise Data Loss Prevention Features

New Enterprise DLP Feature	Description
Enterprise Data Loss Prevention (DLP)	To protect against unauthorized access, misuse, extraction, and sharing of sensitive information, you need to effectively filter network traffic to block or generate an alert before sensitive information leaves the network. Enterprise Data Loss Prevention (DLP) provides a single engine for accurate detection and consistent policy enforcement for sensitive data at rest and in motion. Panorama and managed firewalls running PAN-OS 10.0.2 and later releases support Enterprise DLP.

Ex. 42 at 7, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-release-notes/pan-os-release-notes.pdf.



Ex. 29 at 39-41, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

303. Moreover, the '380 Accused Products set up cloud-based DNS Security Service to access an infinitely scalable DNS signature and protection sources to defend against malicious domains. The DNS security service operates real-time DNS request analysis using predictive analytics and machine learning on multiple DNS sources. Further, DNS Security Service to detect Command and Control Domains (C2) which include URLs (e.g. **HTTP**) and domains used by malware and/or compromised systems to communicate with an attacker's remote server to exfiltrate data. As shown below, the DGA detection prevents data exfiltration by identifying and blocking a domain generated in large amount by a machine. The DNS tunnel detection prevents data exfiltration hidden in the DNS queries and responds through policy rules.

- **Command and Control Domains**—C2 include URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data (this includes DNS tunneling detection and DGA detection).
  - **DNS Tunnel Detection**—DNS tunneling can be used by attackers to encode data of non-DNS programs and protocols within DNS queries and responses. This provides attackers with an open back channel with which they can transfer files or remotely access the system. DNS tunnel detection uses machine learning to analyze the behavioral qualities of DNS queries, including n-gram frequency analysis of domains, entropy, query rate, and patterns to determine if the query is consistent with a DNS tunneling-based attack. Combined with the firewall's automated policy actions, this allows you to quickly detect C2 or data theft hidden in DNS tunnels and to automatically block it, based on your defined policy rules.
  - **DGA Detection**—Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values. While most domains generated by a DGA do not resolve as a valid domain, they must all be identified to fully defend against a given threat. DGA analysis determines whether a domain is likely to have been generated by a machine, rather than a person, by reverse-engineering and analyzing other frequently used techniques found in DGAs. Palo Alto Networks then uses these characteristics to identify and block previously unknown DGA-based threats in real-time.

Ex. 38 at 741, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf.

304. The Accused Products will detect the anomalies in the HTTP requests to malicious hosts that intend to exfiltrate data through DNS traffic. Once the malicious hosts are identified, the Accused Products conduct verification through data exchanges between the requestors and the malicious hosts. As shown below, the Accused Products will either block all unknown applications and traffic using the security policy or direct exfiltration to a "sinkhole," a designated IP tunnel to steer away from malicious domains.

- Block all unknown applications and traffic using the Security policy. Typically, the only applications classified as unknown traffic are internal or custom applications on your network and potential threats. Unknown traffic can be either non-compliant applications or protocols that are anomalous or abnormal or it can be known applications that are using non-standard ports, both of which should be blocked. See Manage Custom or Unknown Applications.

Ex. 38 at 728, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf.

Palo Alto Networks customers are protected in the following ways:

- All RDAT samples have malicious verdicts in WildFire and have protections in place through Cortex XDR.
- DNS tunneling protocols used for C2 communications are blocked via DNS Security.
- All C2 domains are classified as Command-and-Control for URL Filtering.
- AutoFocus customers can monitor activity via the rdat_backdoor tag.

Ex. 43 at 18, https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/.

305. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

306. PAN has willfully infringed the '380 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '380 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

307. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '380 Patent.

308. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

309. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '380 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '380 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '380 Patent, justifying an award to

Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

310. PAN's infringement of the '380 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

311. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

312. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SIXTEENTH CAUSE OF ACTION
(Indirect Infringement of the '380 Patent)

313. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

314. PAN has induced and continues to induce infringement of one or more claims of the '380 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '380 Patent under 35 U.S.C. § 271(c).

315. PAN has induced infringement of the '380 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is

inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '380 Patent, including Claims 1, 6-8, 10-13, 16-19, 21-22, and 25-27.

316. PAN has knowingly and actively aided and abetted the direct infringement of the '380 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '380 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '380 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '380 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '380 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '380 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

317. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '380 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the

operation of the '380 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

318. PAN contributorily infringes the '380 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '380 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The'380 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '380 Patent, including Claims 1, 6-8, 10-13, 16-19, 21-22, and 25-27.

319. PAN has knowingly and actively contributed to the direct infringement of the '380 Patent by its manufacture, use, offer to sell, sale and importation of the '380 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '380 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and

methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

320. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

321. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '380 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '380 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '380 Patent.

322. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SEVENTEENTH CAUSE OF ACTION
(Direct Infringement of the '899 Patent pursuant to 35 U.S.C. § 271(a))

323. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

324. PAN has infringed and continues to infringe a least Claims 1-3, 5-8, 10-16, and 19-20 of the '899 Patent.

325. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

326. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

327. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '899 Patent, these products, services, and technologies including, but not limited to the marketing names: Cortex (the "'899 Accused Products"). PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

328. The '899 Accused Products embody the patented invention of the '899 Patent and infringe the '899 Patent because they include software that causes them to receive a plurality of event logs; determine a reportability likelihood for each event log based on at least one algorithm, wherein the reportability likelihood for each event log is based on at least one of: a fidelity of an event threat indicator, a type of the event threat indicator, an age of the event threat indicator, threat intelligence provider data associated with the event threat indicator, reputation data of at least one threat intelligence provider, or a risk score of the event threat indicator; sort the plurality of event logs based on the reportability likelihood of each of the plurality of event logs; and store, in an event queue, the plurality event logs sorted in the event queue based on the reportability likelihood of each of the plurality of event logs.

329. The '899 Accused Products are software that runs on PAN's cloud servers. For example, Cortex can ingest event logs from a number of different sources, and store this information in its "data lake." Cortex normalizes these event logs and uses advanced machine

learning to determine if reportability likelihood based on factors relate to a score, such as traffic statistics, reputation, malicious scores, threat intelligence, indicators of compromise, Dbot scores, and threat action playbooks.

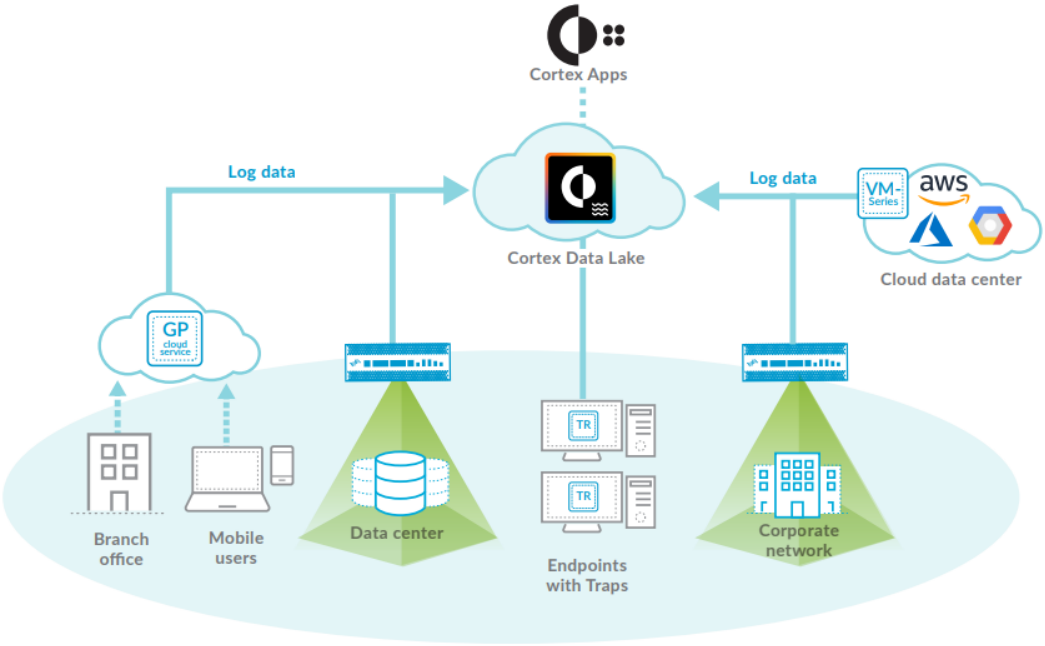


Figure 2: Cortex Data Lake integration

Ex. 23, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

330. The '899 Accused Products store the event logs in a manner sorted by a reportability likelihood, including the severity of the event. For example, Cortex sorts event logs based on machine learning algorithms that identify events with the highest risk (e.g., reportability likelihood) associated with them. These sorted event logs are stored in queue that prioritizes the event with the highest risk associated with it, which allows the event to be addressed using a ticketing or automation system.

331. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

332. PAN has willfully infringed the '899 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '899 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

333. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '899 Patent.

334. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

335. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '899 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '899 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '899 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

336. PAN's infringement of the '899 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

337. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

338. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

EIGHTEENTH CAUSE OF ACTION
(Indirect Infringement of the '899 Patent)

339. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

340. PAN has induced and continues to induce infringement of one or more claims of the '899 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '899 Patent under 35 U.S.C. § 271(c).

341. PAN has induced infringement of the '899 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '899 Patent, including Claims 1-3, 5-8, 10-16, and 19-20.

342. PAN has knowingly and actively aided and abetted the direct infringement of the '899 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '899 Patent with the Accused

Products. Such use is consistent with how the products are described to directly infringe the '899 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '899 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '899 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '899 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

343. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the ''899 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '899 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

344. PAN contributorily infringes the '899 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '899 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '899 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '899 Patent, including Claims 1-3, 5-8, 10-16, and 19-20.

345. PAN has knowingly and actively contributed to the direct infringement of the '899 Patent by its manufacture, use, offer to sell, sale and importation of the '899 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '899 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

346. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

347. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '899 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '899 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '899 Patent.

348. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

NINETEENTH CAUSE OF ACTION
(Direct Infringement of the '906 Patent pursuant to 35 U.S.C. § 271(a))

349. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

350. PAN has infringed and continues to infringe a least Claims 1-3, 5-10, 11-15, and 17 of the '906 Patent.

351. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

352. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

353. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '906 Patent, these products, services, and technologies including, but not limited to the

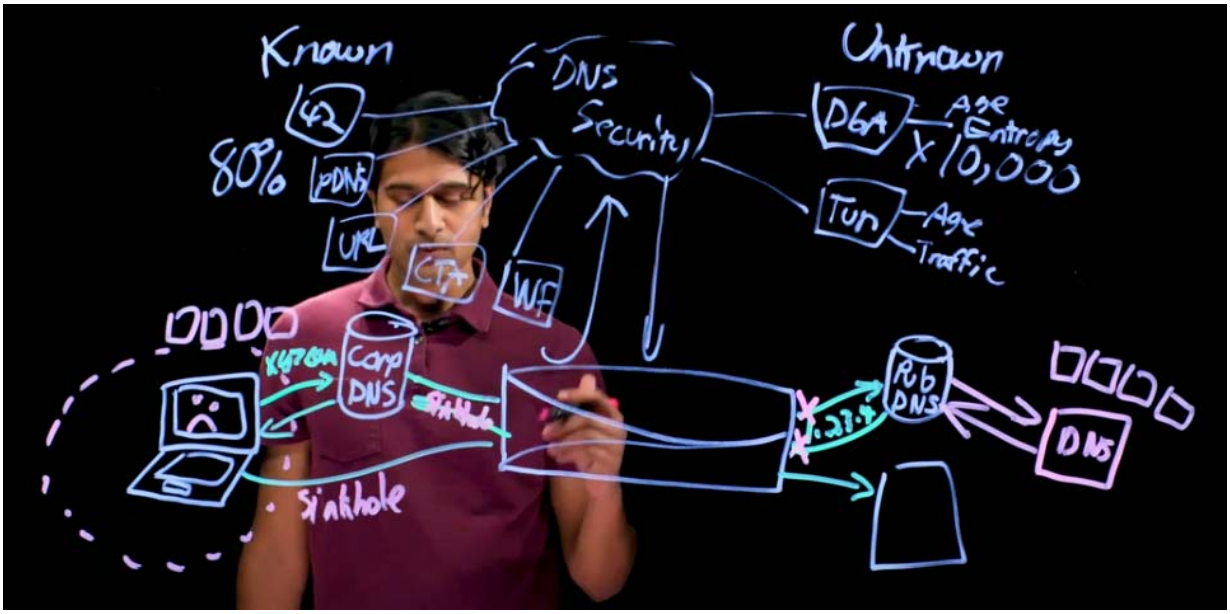
marketing names: NGFW and/or DNS Security Service (the "'906 Accused Products"). Combinations of the '906 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, NGFW alone or in combination with DNS Security Service, infringe the '906 Patent. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

354. The '906 Accused Products embody the patented invention of the '906 Patent and infringe the '906 Patent because they perform receiving, by a packet security gateway, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server, wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and wherein one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service; performing, on a packet by packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets, wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest

logging function that supports a network communications awareness service and comprises: identifying a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function; generating a record comprising the subset of information specified by the packet; reformatting the subset of information specified by the packet in accordance with a logging system standard; and routing, by the packet security gateway, the packet to a monitoring device; receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules and was generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service; and performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules.

355. The ‘906 Accused Products include a packet security gateway because the NGFW operates as a gateway to enforce security protocols related to all network traffic entering and exiting a networks at an organization at the packet level. As shown below, the NGFW is associated with a security policy management server in the form of the DNS Security Service, a service that is managed on a separate network. The NGFW receives packet filtering rules from the DNS Security Service. This includes “real-time” lookups to determine if a DNS query is to a known malicious domain. The dynamic security policy will include information on whether the lookup should cause the creation of a “sinkhole”. The “sinkhole” is created by

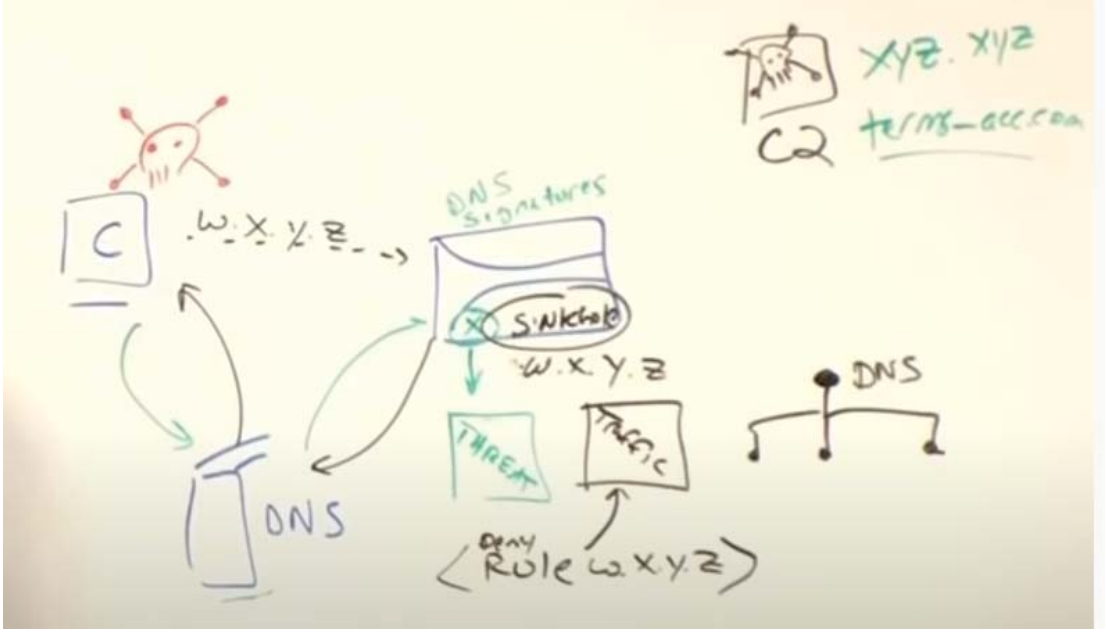
sending a custom IP address to the user requesting the malicious domain and traffic to be stored in a traffic log.



https://www.youtube.com/watch?v=ux61BJudJW8.

356. For example, the DNS Security Service incorporates multiple different "malicious host trackers" into its analysis.

357. Additionally, the '906 Accused Products receive packets from clients that are contained within a protected network, and are therefore associated with the network. For example, the NGFW will have packet filtering rules associated with the real time DNS security service lookup. As shown below, the packet transformation functions include sending the traffic to a sinkhole and logging the resulting traffic so that the infected client can be identified.



https://www.youtube.com/watch?v=FUFtEEMEE00.

358. Additionally, the '906 Accused Products use a packet digest logging function will identify a subset of information specified by the packet in the form of the user that has attempted to contact the sink hole, record the contacts he makes, and reformat the information using logging system standards, such as NetFlow. As shown below, the packet digest logging function will identify a subset of information specified by the packet in the form of the user that has attempted to contact the sink hole and will record the contacts he makes.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	06/21 12:08:08	drop	L3-trust	L3-untrust	192.168.45.147		72.5.65.111	0	ping	deny	block-dns-sinkhole	policy-deny	148
	06/21 12:07:59	drop	L3-trust	L3-untrust	192.168.45.147		72.5.65.111	0	ping	deny	block-dns-sinkhole	policy-deny	148
	06/21 12:02:28	drop	L3-trust	L3-untrust	192.168.45.147		72.5.65.111	0	ping	deny	block-dns-sinkhole	policy-deny	74

https://www.youtube.com/watch?v=WWU_tt3YzZk.

359. The system will route the packets based on information in the packet. The DNS Security Server updates the packet filtering rules on the NGFW with new sets of information, including new rules through dynamic lookups, based at least in part on updates to the malicious

traffic information from the malicious host trackers. The NGFW will perform packet filtering on subsequent packets based on the updated DNS Security rules.

360. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

361. PAN has willfully infringed the '906 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '906 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

362. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '906 Patent.

363. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

364. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '906 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '906 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '906 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

365. PAN's infringement of the '906 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

366. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

367. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTIETH CAUSE OF ACTION
(Indirect Infringement of the '906 Patent)

368. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

369. PAN has induced and continues to induce infringement of one or more claims of the '906 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '906 Patent under 35 U.S.C. § 271(c).

370. PAN has induced infringement of the '906 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '906 Patent, including Claims 1-3, 5-10, 11-15, and 17.

371. PAN has knowingly and actively aided and abetted the direct infringement of the '906 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '906 Patent with the Accused

Products. Such use is consistent with how the products are described to directly infringe the '906 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '906 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '906 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '906 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

372. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '906 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '906 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

373. PAN contributorily infringes the '906 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '906 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '906 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '906 Patent, including Claims 1-3, 5-10, 11-15, and 17.

374. PAN has knowingly and actively contributed to the direct infringement of the '906 Patent by its manufacture, use, offer to sell, sale and importation of the '906 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '906 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

375. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

376. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '906 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '906 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '906 Patent.

377. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-FIRST CAUSE OF ACTION
(Direct Infringement of the '246 Patent pursuant to 35 U.S.C. § 271(a))

378. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

379. PAN has infringed and continues to infringe a least Claims 1-20 of the '246 Patent.

380. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

381. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

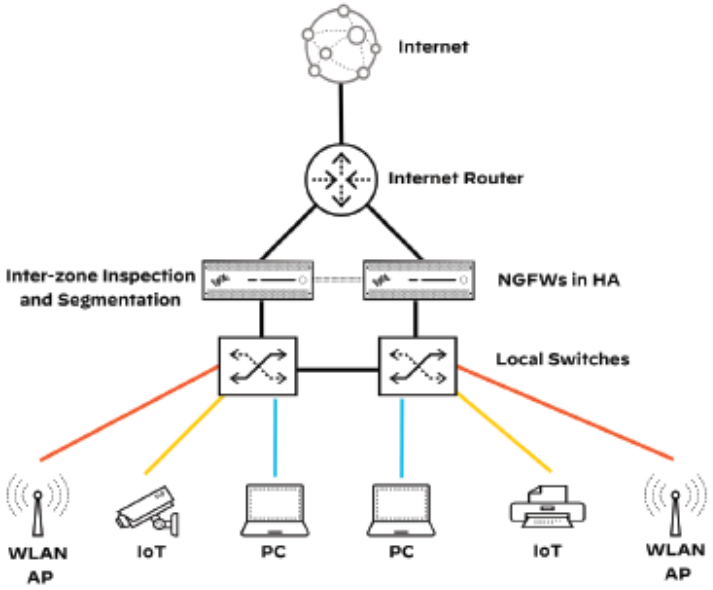
382. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '246 Patent, these products, services, and technologies including, but not limited to the

marketing names: NGFW, Cortex, AutoFocus, and/or MineMeld (the "'246 Accused Products"). Combinations of the '246 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '246 Accused Products infringe under at least the following scenarios: (1) NGFW and (2) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus or MineMeld. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

383. The '246 Accused Products embody the patented invention of the '246 Patent and infringe the '246 Patent because they include at least one processor; and a memory storing instructions that when executed by the at least one processor cause the network security device to: receive, at the network security device, a plurality of rule sets; receive a plurality of packets via a communication interface of the network security device; execute, at a first time and on a packet by packet basis, a first rule set specifying a first set of network addresses for which packets should be forwarded; execute, at a second time and on a packet by packet basis, a second rule set specifying a second set of network addresses for which packets should be forwarded; and execute, at a third time and on a packet by packet basis, a third rule set specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses,

and the third set of network addresses including more network addresses than the second set of network addresses.

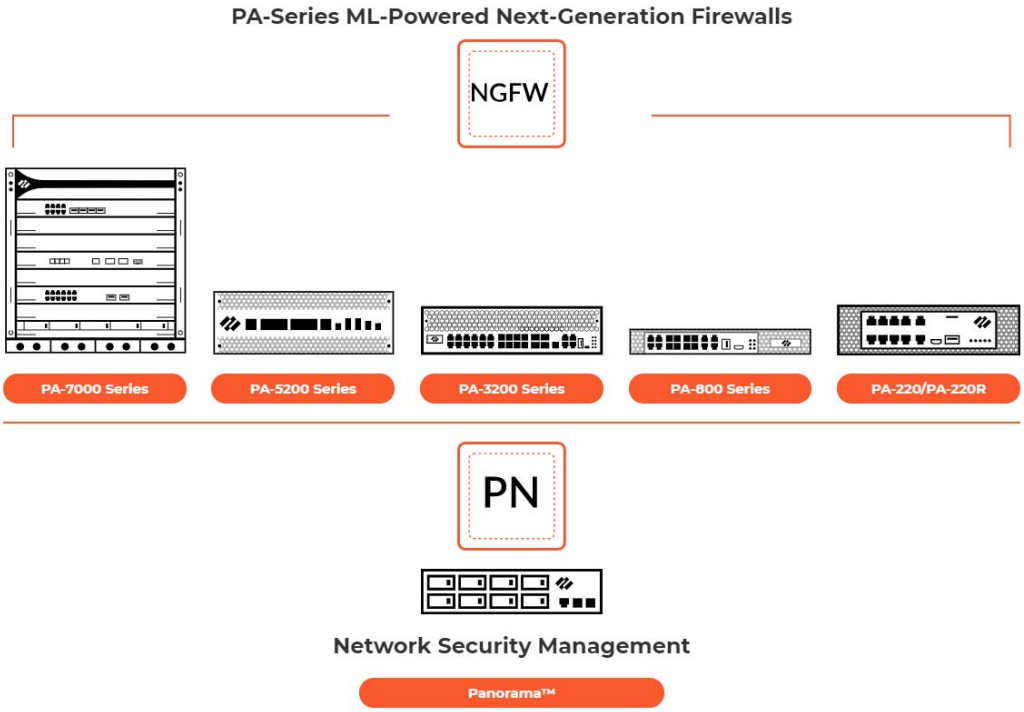
384. The '246 Accused Products are packet security gateways that protect organizations and data centers at the network perimeter. The '246 Accused Products run on computer systems with a processor, main memory, and RAM. The memory stores the instructions that are executed by the processor.



Ex. 29 at 27-28, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

385. For example, Panorama provisions one or more of the NGFW with packet filtering rules applied to all traffic traversing a network boundary. The NGFW(s) deployed in a network collectively provide an interface across a boundary of the network and implement a "zero trust" system were all traffic must be validated and may block or allow traffic based on rules. Additionally, the '246 Accused Products, integrate logs, malware analysis reports, and visibility into malicious events, including by using PAN-OS, Panorama network security management, AutoFocus contextual threat intelligence service, Cortex XSOAR, and Cortex

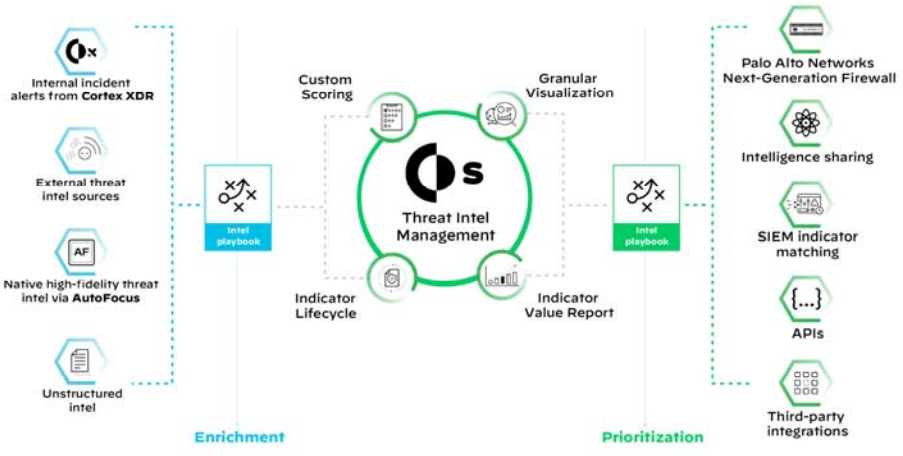
XDR. As an example, Panorama includes AutoFocus threat feeds, which include IP addresses, domains, URLs, and hash indicators and is continually updated. Additionally, AutoFocus includes a threat intelligence analysis database (including information from multiple sources like WildFire, Unit 42, and third party feeds) that create rules (e.g. threat feed or threat indicators) which are provisioned to packet-filtering devices (e.g. NGFW) using MineMeld. Panorama and NGFW also includes independent network-threat-intelligence providers (supported threat feed sources).



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

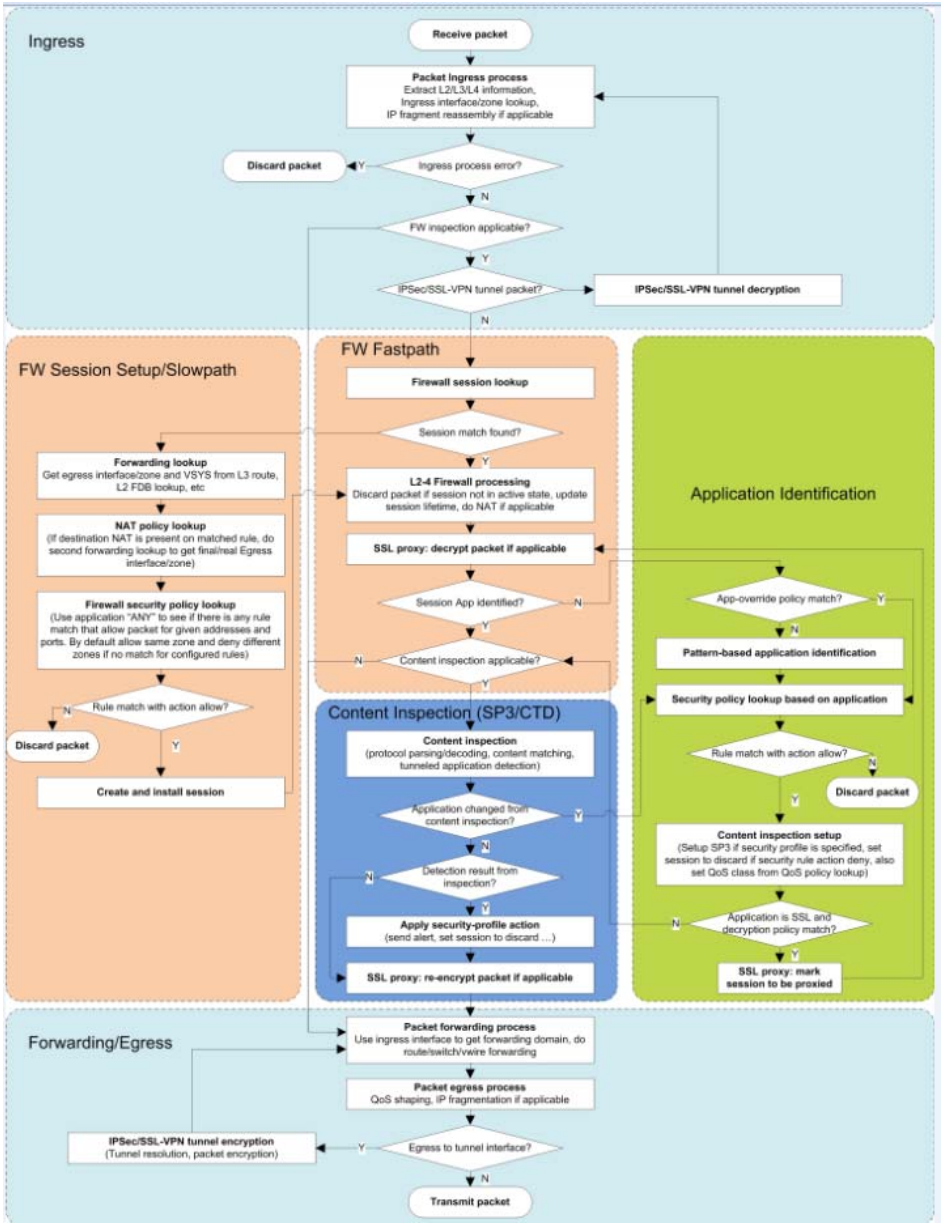
386. Additionally, the NGFW is provisioned with dynamic security policies with packet filtering rules, such as create block/accept policies (Source, Destination, Port), for IP addresses and domains in the PAN-OS firewalls, from Cortex, which is a security policy management server. The packet filtering rules identify packets corresponding to network

threat indicators, which are associated with network-threat-intelligence reports from independent providers.



Ex. 28, https://www.paloaltonetworks.com/cortex/threat-intel-management.

387. Further, the '246 Accused Products receive all traffic traversing the network and applies a single-pass architecture, which processes each packet, including for policy lookup, decoding, threat detection, content checking, application checking, and networking. For example, the NGFW will inspect all incoming and outgoing packets, allowing Panorama to aggregates logs from all managed firewalls and provides visibility across all the traffic on the network.



Ex. 37,

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.

388. The '246 Accused Products are automatically updated with new rules that are applied to subsequent packets. For example, Panorama will update the NGFW as new threat information is made available from the utilized threat services.

389. The '246 Accused Products will apply rule sets that are prioritized based on their location in a network, with different sets of rules based on the origination and destination of the packet. Furthermore, the '246 Accused Products include local firewall rules, device group post-rules, and shared post-rules that are evaluated in order with later rule sets which have more rules than the previous. The rule sets include a set of network addresses which should be forwarded, with each rule set including more rules (e.g., network addresses) than the previous rule sets. The rule sets are executed at different points in time, with the smaller rule set being executed first, followed by a larger rule set, and then an even larger rule set, which allows higher priority network traffic to be processed before lower priority traffic.

390. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

391. PAN has willfully infringed the '246 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '246 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

392. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '246 Patent.

393. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

394. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '246 Patent to avoid infringement despite PAN's

knowledge and understanding that its products and services infringe the '246 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '246 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

395. PAN's infringement of the '246 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

396. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

397. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-SECOND CAUSE OF ACTION
(Indirect Infringement of the '246 Patent)

398. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

399. PAN has induced and continues to induce infringement of one or more claims of the '246 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '246 Patent under 35 U.S.C. § 271(c).

400. PAN has induced infringement of the '246 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are

used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '246 Patent, including Claims 1-20.

401. PAN has knowingly and actively aided and abetted the direct infringement of the '246 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '246 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '246 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to, advising third parties to use the '246 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '246 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '246 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

402. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '246 Accused Products in an infringing

manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '246 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

403. PAN contributorily infringes the '246 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '246 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '246 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it was contributing to the infringement of one or more claims of the '246 Patent, including Claims 1-20.

404. PAN has knowingly and actively contributed to the direct infringement of the '246 Patent by its manufacture, use, offer to sell, sale and importation of the '246 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '246 Patent, as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in

the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

405. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

406. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '246 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '246 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '246 Patent. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-THIRD CAUSE OF ACTION
(Direct Infringement of the '413 Patent pursuant to 35 U.S.C. § 271(a))

407. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

408. PAN has infringed and continues to infringe a least Claims 1-20 of the '413 Patent.

409. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

410. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

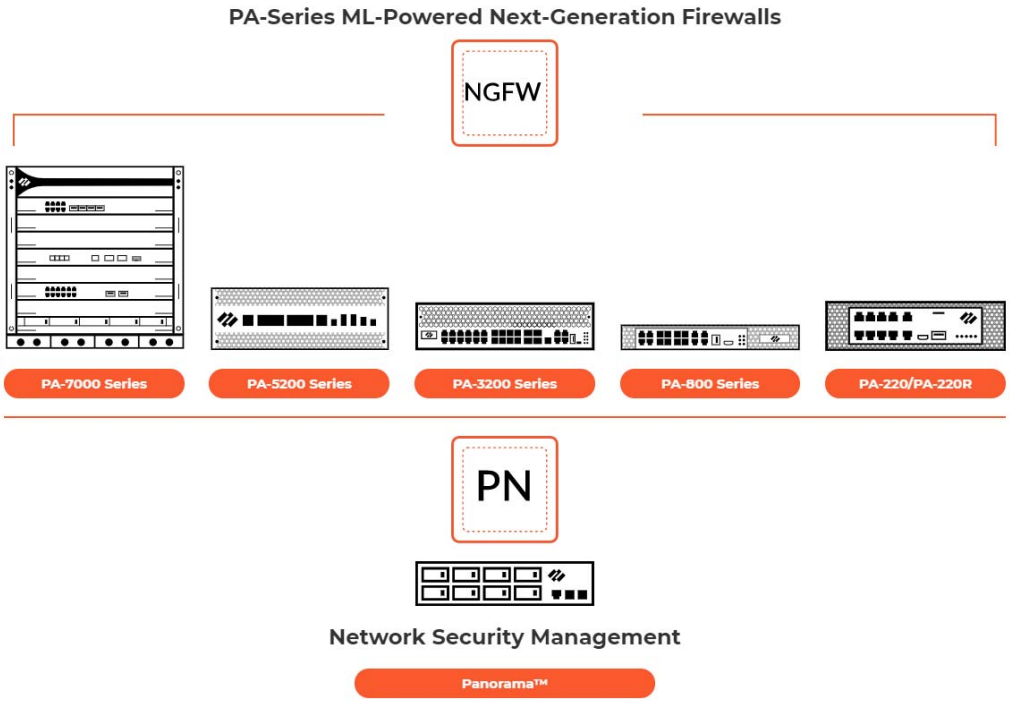
411. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '413 Patent, these products, services, and technologies including, but not limited to the marketing names: NGFW, Panorama, Cortex, AutoFocus, MineMeld, and/or DNS Security Service (the "'413 Accused Products"). Combinations of the '413 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, the '413 Accused Products infringe under at least the following scenarios: (1) NGFW, (2) NGFW and Panorama, (3) NGFW, Panorama, and Cortex, (4) NGFW and Cortex, with any of the scenarios alone or in combination with AutoFocus, MineMeld or DNS Security. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

412. The '413 Accused Products embody the patented invention of the '413 Patent and infringe the '413 Patent because they include at least one processor; and memory storing instructions that when executed by the at least one processor cause the packet-filtering device to: receive a plurality of threat identifiers from a plurality of network-threat-intelligence providers; receive a plurality of packets; responsive to a determination by the packet-filtering device that a first packet of the plurality of packets corresponds to a first packet matching criterion specified by a first packet-filtering rule of a plurality of packet-filtering rules: apply, to the first packet, a first operator specified by the first packet-filtering rule corresponding to

the first packet matching criterion; generate, for the first packet, a packet log entry comprising at least one threat identifier, of the plurality of threat identifiers, corresponding to the first packet; determine a number of network-threat-intelligence providers, of the plurality of network-threat-intelligence providers, from which the at least one threat identifier corresponding to the first packet was received; and determine at least one score associated with the at least one threat identifier determining at least a first score based on the determined number of network-threat-intelligence providers; generate a listing of at least a portion of the plurality of threat identifiers, comprising the at least one threat identifier, wherein a position of the at least one threat identifier in the listing is based on the determined first score; and reconfigure at least one packet-filtering rule based on user input received via a user interface comprising at least the generated listing, wherein each of the plurality of packet-filtering rules specifies at least one packet matching criterion and at least one operator.

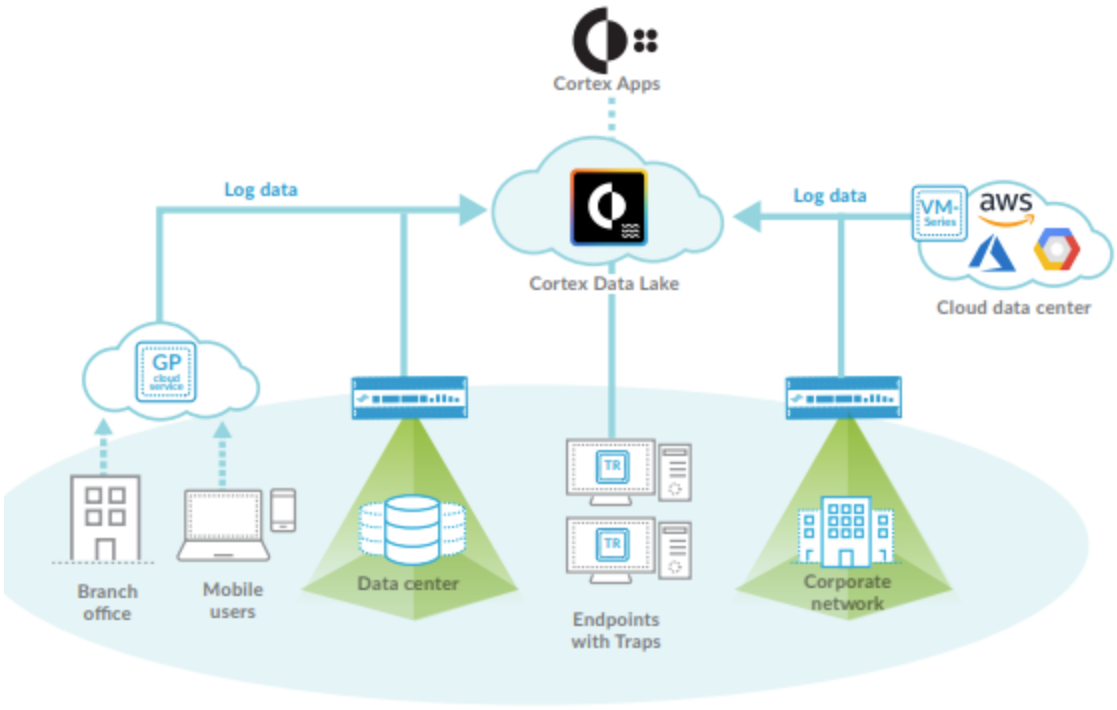
413. For example, with the '413 Accused Products, the NGFW operates at the boundary of a network and receives plurality of filtering rules from Panorama, which is a rule provider device. The packet filtering rules are applied to all traffic traversing the network boundary. Panorama acts as a centralized security management system for global control of the NGFW and provides a single security rule base for threat prevention, URL filtering, application awareness, user identification, and sandboxing. The packet filtering rules are applied to all traffic traversing the network boundary. For example, Panorama, through AutoFocus, provides integrated logs, malware analysis reports, and visibility into malicious events. AutoFocus threat feeds include IP addresses, domains, URLs, and hash indicators that are updated daily and form the packet filtering rules. AutoFocus is a threat intelligence analysis database creates rules which are provisioned to the NGFW using MineMeld and form

the packet filtering rules. Additionally, Panorama provides threat intelligence and network security management using AutoFocus contextual threat intelligence, Cortex (including XSOAR and XDR), that form packet filtering rules. Additionally, AutoFocus includes a threat intelligence analysis database (including information, such as malicious traffic information, from multiple sources like WildFire, Unit 42, and third party feeds) that create rules (e.g. threat feed or threat indicators) which are provisioned to packet-filtering devices (e.g. NGFW) using MineMeld and form the packet filtering rules. Panorama and NGFW also includes independent network-threat-intelligence providers (supported threat feed sources). These packet filtering rules include operators which specify whether the particular packets should be blocked or allowed. The operators can be updated, and therefore modified, based on packet filtering rule updates, which can specify whether to block or allow the packet.



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

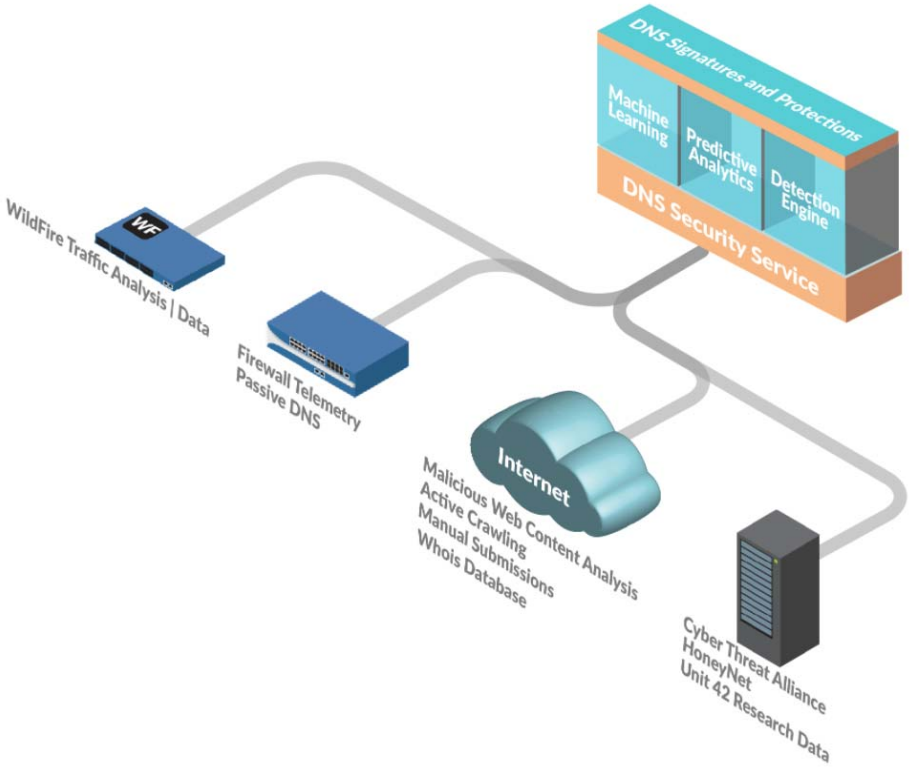
414. As an additional example, the NGFW receives packet filtering rules from Cortex, which is a rule provider device. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers. Shown below, Cortex XDR analyzes network data with machine learning, to pinpoint targeted attacks, malicious insiders and compromised endpoints. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers. The packet filtering rules identify packets corresponding to network threat indicators, which are associated with network-threat-intelligence reports from independent providers.



Ex. 23,

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-data-lake.

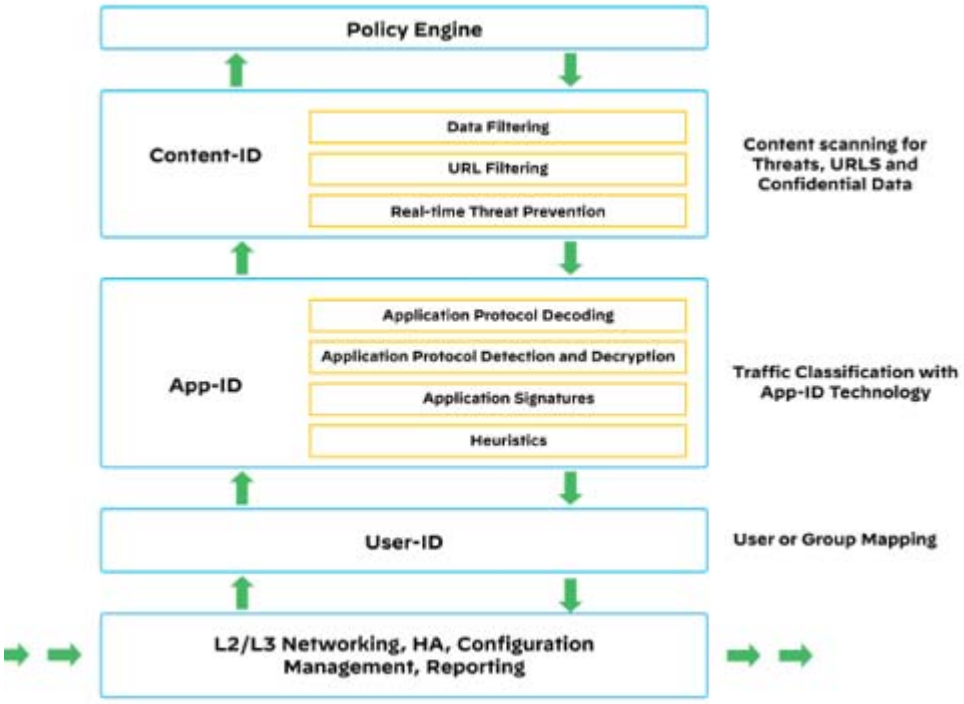
415. Furthermore, the NGFW includes DNS Security Service, which protects and defends from advanced threats using DNS, which leverages advanced machine learning and predictive analytics, to provide real-time DNS request analysis and rapid production of DNS signatures specifically designed to defend against malware using DNS for C2 and data theft. In this way, it provides access to a threat intelligence system to keep your network protections up to date.



Ex. 26, https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/dns-security/about-dns-security.html#par_concept.

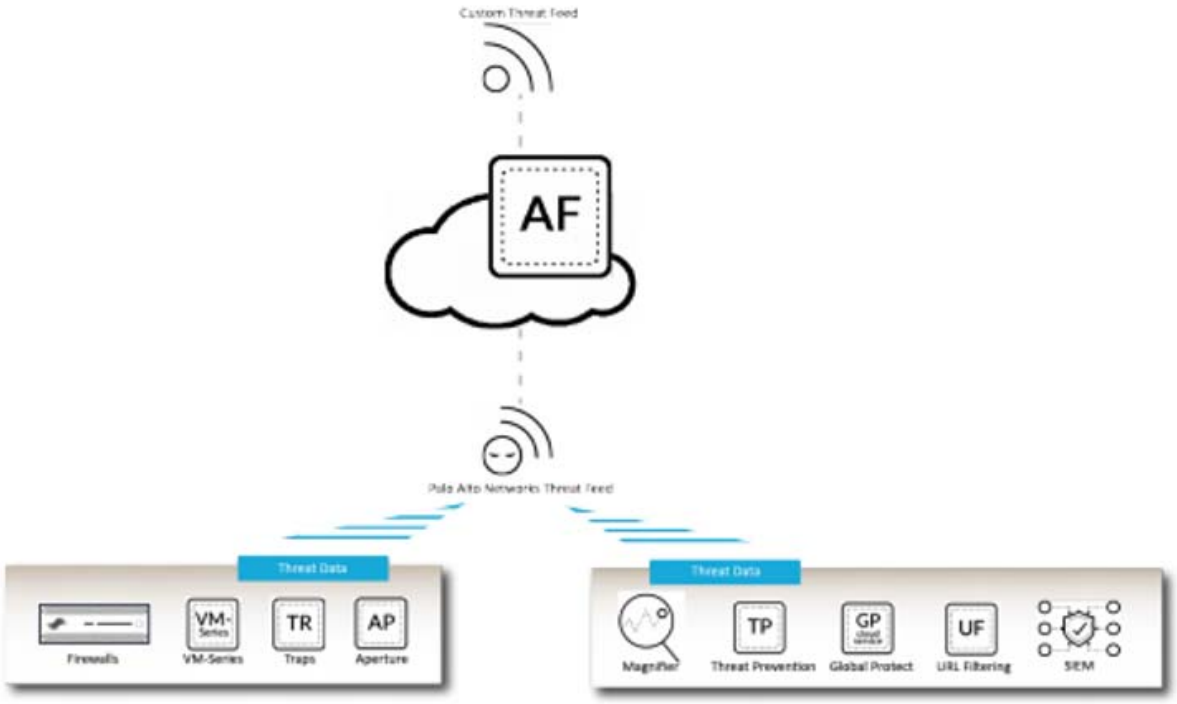
416. The '413 Accused Products use a single-pass architecture, to process each packet, including with policy lookup, decoding, threat detection, content checking, application checking, and networking. The NGFW uses security policy rules as packet-filtering rules and applies them bidirectional traffic, including inbound and outbound packets. The NGFW is also

zone-based and segments where all nodes share similar network security requirements and evaluate traffic as it passes from one zone to another. The NGFW performs packet processing using rules from various policies, including the Security Policy Lookup to allow or deny packets. The NGFW includes DNS Security, which analyzes network packets to determine the packet satisfies the packet filtering rules, such as the DNS Security rules. You can then capture packets for further analysis.



Ex. 29 at 14, https://www.paloaltonetworks.com/resources/guides/network-security-overview.

417. In the '413 Accused Products, information is communicated to Panorama, including whether packets were allowed or blocked. In a further example, Panorama includes AutoFocus threat feeds, which include IP addresses, domains, URLs, and hash indicators that are updated based on the most recent threat information, which can include updating network threat indicators based on the latest threat information. After this update occurs, the '413 Accused Products is updated to operate on subsequent packets with the packet filtering rule.



Ex. 30 at 165, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/autofocus/autofocus-admin/autofocus-admin.pdf.

418. The '413 Accused Products determines an ordering for network threats and analyzes a combination of network metadata to detect advanced attacks. The ordering is based on a score, which is determined at least in part by the number of times the network threat matches with information from multiple threat intelligence providers. For example, Cortex determines receives lists of threats from multiple network threat intelligence providers, which includes rules for identifying network threats based on its Dbot technology, threat intelligence details and artifacts, incident scores, monitoring traffic in the system, and analyzing protocol level metadata traffic logs. The '413 Accused Products generate a list of the network threats and reconfigure packet filtering rules based on input received regarding the list.

419. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

420. PAN has willfully infringed the '413 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '413 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

421. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '413 Patent.

422. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

423. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '413 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '413 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '413 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

424. PAN's infringement of the '413 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

425. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

426. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-FOURTH CAUSE OF ACTION
(Indirect Infringement of the '413 Patent)

427. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

428. PAN has induced and continues to induce infringement of one or more claims of the '413 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '413 Patent under 35 U.S.C. § 271(c).

429. PAN has induced infringement of the '413 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '413 Patent, including Claims 1-20.

430. PAN has knowingly and actively aided and abetted the direct infringement of the '413 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '413 Patent with the Accused

Products. Such use is consistent with how the products are described to directly infringe the '413 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement includes, but is not limited to: advising third parties to use the '413 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a mechanism through which third parties may infringe; by advertising and promoting the use of the '413 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '413 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

431. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '413 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '413 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

432. PAN contributorily infringes the ‘413 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the ‘413 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ‘413 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of others for one or more claims of the ‘413 Patent, including Claims 1-20.

433. PAN has knowingly and actively contributed to the direct infringement of the ‘413 Patent by its manufacture, use, offer to sell, sale and importation of the ‘413 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the ‘413 Patent, as described above and is incorporated by reference. Furthermore, PAN’s customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN’s ability to provide security and protection and identify threats across its customer base.

434. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

435. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '413 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '413 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '413 Patent.

436. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-FIFTH CAUSE OF ACTION
(Direct Infringement of the '797 Patent pursuant to 35 U.S.C. § 271(a))

437. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

438. PAN has infringed and continues to infringe a least Claims 1-9 and 11-20 of the '797 Patent.

439. PAN's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

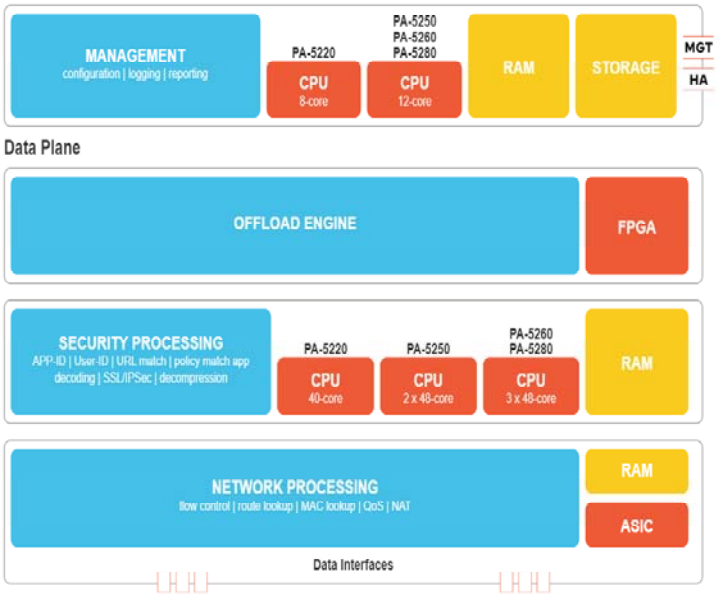
440. PAN's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

441. PAN's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '797 Patent, these products, services, and technologies including, but not limited to the

marketing names: NGFW and/or Cortex (the "'797 Accused Products"). Combinations of the '797 Accused Products infringe in a similar manner as described in the examples set forth herein. For example, NGFW and Cortex, separately or in combination, infringe the '797 Patent. PAN also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of PAN, to the extent specific components are provided by those customers or vendors. PAN directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, PAN put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

442. The '797 Accused Products embody the patented invention of the '797 Patent and infringe the '797 Patent because they determine a first plurality of log entries corresponding to a plurality of packets received by a network device from a first host located in a first network; determine a second plurality of log entries corresponding to a plurality of packets transmitted by the network device to a second host located in a second network; correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device by comparing at least a first portion of the first plurality of log entries with at least a second portion of the second plurality of log entries; generate, based on the correlating, one or more rules configured to identify packets received from the first host; and provision a packet-filtering device with the one or more rules.

443. For example, as shown below, the '797 Accused Products include at least one processor and memory comprising instructions that, when executed by the at least one processor, cause a computing device to perform functionalities.



Ex. 18, https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures.

444. For instance, Cortex XDR is used to "[d]etect targeted attacks, insider threats, and malware with AI-powered analytics" and "monitor internet traffic as well as internal, east-west communications between your users and servers to detect post-intrusion activity, such as lateral movement and exfiltration."

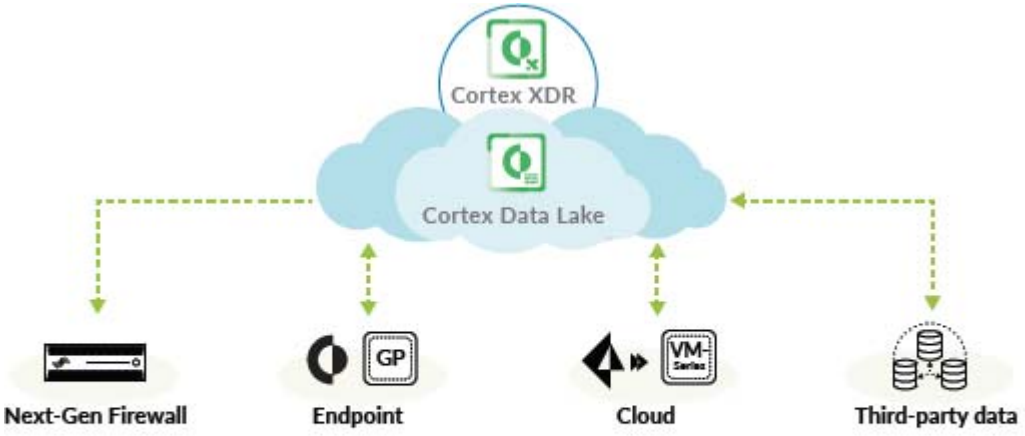
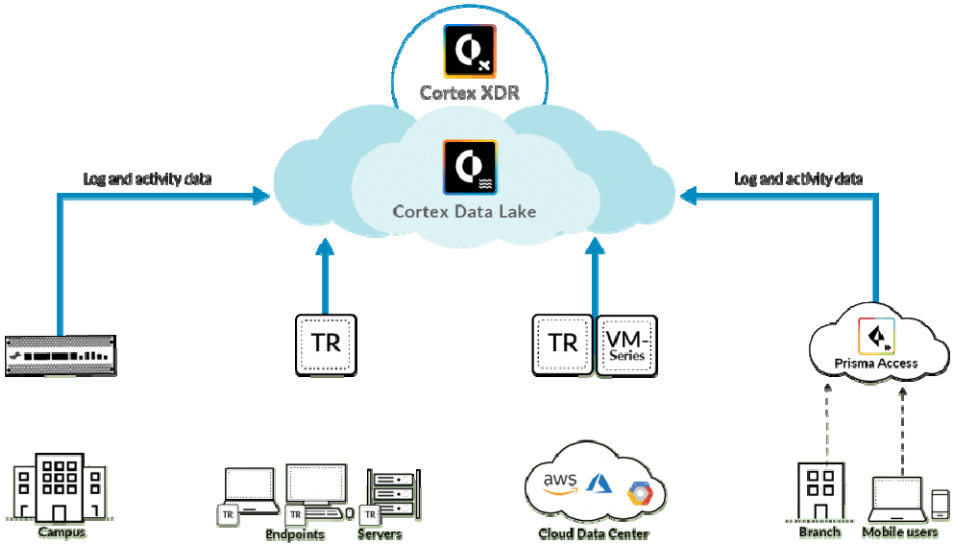


Figure 2: Cortex XDR with one or more data sources for detection and response, eliminating blind spots

Ex. 32 at 1-2, https://live.paloaltonetworks.com/twzvq79624/attachments/twzvq79624/members_discuss/84686/1/Cortex_XDR-NTA.pdf;

Ex. 33 at 26, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf.

445. The NGFW generates log and activity data, based on the network traffic, which are collected and stored in the cloud-based Cortex Data Lake for analysis.



Ex. 34, https://paloaltofirewalls.co.uk/cortex-xdr-managed-detection-and-response/.

446. The '797 Accused Products "monitors internal traffic as well as outbound traffic from clients and servers to the internet" and build profiles from the logs based on "frequency of connections," test periods (e.g. 10 minutes or "10 KB or more were sent encoded in subdomain names during a 10-minute window") as well as the number of endpoints in your network that access certain domains "over time." Ex. 35 at 5, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan

/en_US/resources/whitepapers/stop-targeted-attacks-without-decrypting-traffic; Ex. 44 at 21, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference.pdf.

447. The '797 Accused Products determines differences in transmission and receipt times in detecting attack tactics. For example, it detects the discovery tactic "by looking for symptoms in your internal network traffic such as changes in connectivity patterns that including increased rates of connections." In another, it detects whether an endpoint is controlled by a command and control server by looking "for anomalies in outbound connections" and "for unexplained changes in the periodicity of connections." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

448. The '797 Accused Products uses an analytics engine to correlate and compare data by examining logs and data from your sensors. The analytics engine retrieves logs from Cortex Data Lake to understand the normal behavior (creates a baseline) so that it can raise alerts when abnormal activity occurs. Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

449. The '797 Accused Products also uses Log Stitching and the Causality Analysis Engine to correlate and compare logs and event data to establish causality chains that identify the root cause, including identifying "a complete forensic timeline of events that helps you to determine the scope and damage of an attack" and "the sequence of activity that led to the alert." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html; Ex. 45, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xdr/cortex-

xdr-pro-admin/cortex-xdr-pro-admin.pdf. The '797 Accused Products generate rules to identify suspicious activity, such as traffic received from a suspicious network host, and provision packet filtering devices with the rules.

450. The '797 Accused Products analyze the data the NGFW collects and generate "an analytics alert when the analytics engine determines an anomaly…and use alerts to notify you of that abnormal behavior." The '797 Accused Products use the analytics engine to "examine traffic and data from a variety of sources such as network activity from firewall logs …to identify endpoints and users on your network." Ex. 36, https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/analytics/analytics-concepts.html.

ıdpoint and net-
ex XDR can pin-
malware. It can
us sequences of
endpoint, such
o shut down an
ication, suspi-
ations, registry
re than a hundred other signs of malware and
ndpoint. With behavioral analytics, it can also
-based malware activity.

Focus on Network-Level Information, Not Application Contents

To detect attacks from unmanaged devices, Cortex XDR primarily inspects network metadata, such as traffic source, destination, domain, protocol, port number, and volume, which can be obtained from packet headers even when application-level content is encrypted.

Cortex XDR analyzes data Next-Generation Firewalls collect to track the normal behavior of users and devices, including the systems they access, the protocols they use, the amount of traffic they send and receive, and more. If Cortex XDR detects anomalous activity, it will generate an alert. Because it can detect attacks without inspecting application contents, application-level encryption does not affect detection (see figure 3).

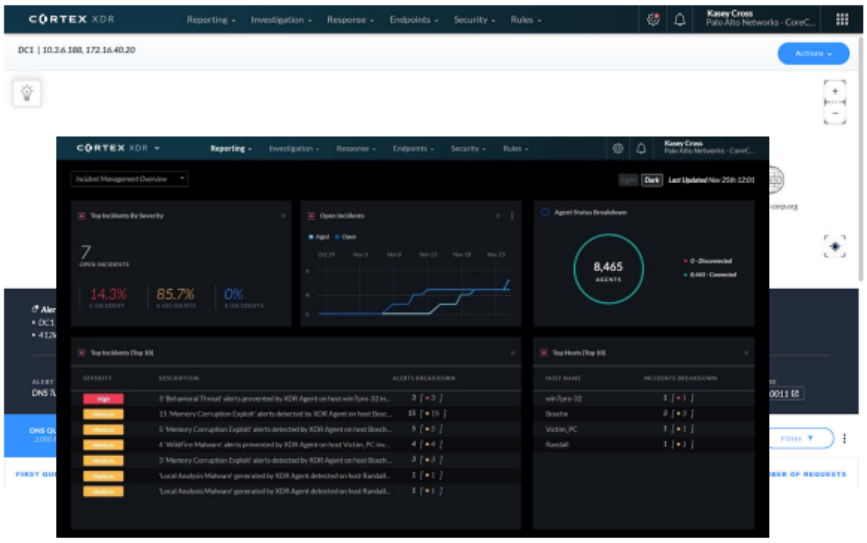


Figure 3: Cortex XDR detects network port scans even if individual requests are encrypted

Ex. 35 at 4,

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/stop-targeted-attacks-without-decrypting-traffic.

451. As a result of PAN's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

452. PAN has willfully infringed the '797 Patent. As discussed above in Paragraphs 65-77, Centripetal is informed and believes that PAN had knowledge of the '797 Patent

through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

453. PAN thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '797 Patent.

454. Despite this knowledge and/or willful blindness, PAN has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

455. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '797 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '797 Patent. As such, PAN has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '797 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

456. PAN's infringement of the '797 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

457. PAN's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

458. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-SIXTH CAUSE OF ACTION
(Indirect Infringement of the '797 Patent)

459. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

460. PAN has induced and continues to induce infringement of one or more claims of the '797 Patent under 35 U.S.C. § 271(b). PAN has contributorily infringed and continues to contributorily infringe of one or more claims of the '797 Patent under 35 U.S.C. § 271(c).

461. PAN has induced infringement of the '797 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and/or manufacturers to perform one or more of the steps of the method claims, or provide one or more component of a system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used either PAN, its customers, purchasers, users, developers, vendors, and/or manufacturers or some combination thereof. PAN has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with PAN, one or more claims of the '797 Patent, including Claims 1-9 and 11-20.

462. PAN has knowingly and actively aided and abetted the direct infringement of the '797 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '797 Patent with the Accused Products. Such use is consistent with how the products are described to directly infringe the '797 Patent and how they are intended to be used, as described above and is incorporated by reference. PAN's specific intent to encourage infringement, but is not limited to: advising third parties to use the '797 Accused Products in an infringing manner through direct communications with third parties via training, support services, or sales calls, providing a

mechanism through which third parties may infringe; by advertising and promoting the use of the '797 Accused Products in an infringing manner; and distributing guidelines and instructions to third parties on how to setup the '797 Accused Products in an infringing manner. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to benefit its ability to provide security and protection and, identify threats across its customer base.

463. PAN updates and maintains an HTTP site called "TECHDOCS" that includes technical documentation encouraging the use of the '797 Accused Products in an infringing manner. This technical documentation includes a knowledge base, videos, getting started guides, administration guides, best practices guides, and deployment guides that cover the operation of the '797 Accused Products in-depth, including by advertising the Accused Products' infringing security features and instructing customers, purchasers, users, developers, vendors, and/or manufacturers to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 31, https://docs.paloaltonetworks.com/.

464. PAN contributorily infringes the '797 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of claims of the '797 Patent. In particular, PAN knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '797 Accused Products are highly developed and specialized security products, and are not staple articles or commodities of commerce because they are specifically made to be

used in an infringing manner, as described in the direct infringement claim above. PAN has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '797 Patent, including Claims 1-9 and 11-20.

465. PAN has knowingly and actively contributed to the direct infringement of the '797 Patent by its manufacture, use, offer to sell, sale and importation of the '797 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '797 Patent as described above and is incorporated by reference. Furthermore, PAN's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with PAN, to the extent specific components are provided by those third parties. To the extent PAN's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, PAN obtains benefits from the control of the system as a whole. PAN and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of PAN's ability to provide security and protection and identify threats across its customer base.

466. PAN's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

467. PAN has known or, in the alternative, has been willfully blind to Centripetal's technology and the '797 Patent. Centripetal is informed and believes that PAN has undertaken no efforts to design these products or services around the '797 Patent to avoid infringement despite PAN's knowledge and understanding that its products and services infringe the '797 Patent.

468. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Centripetal prays for relief and judgment as follows:

(A) An entry of judgment holding that PAN has infringed and is infringing the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413, and '797 Patent.

(B) A preliminary and permanent injunction against PAN and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413, and '797 Patent.

(C) An award to Centripetal of such damages as it shall prove at trial against PAN that is adequate to fully compensate Centripetal for PAN's infringement of the '028 Patent, '126 Patent, '903 Patent, '573 Patent, '437 Patent, '266 Patent, '343 Patent, '380 Patent, '899 Patent, '906 Patent, '246 Patent, '413, and '797 Patent.

(D) A determination that PAN's infringement has been willful, wanton, deliberate, and egregious;

(E) A determination that the damages against PAN be trebled or for any other basis within the Court's discretion pursuant to 35 U.S.C. § 284;

(F) A finding that this case is "exceptional" and an award to Centripetal of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

(G) An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the '028 Patent, '126

Patent, ‘903 Patent, ‘573 Patent, ‘437 Patent, ‘266 Patent, ‘343 Patent, ‘380 Patent, ‘899 Patent, ‘906 Patent, ‘246 Patent, ‘413, and ‘797 Patent.

(H) Such further and other relief as the Court may deem proper and just.

Respectfully submitted,

Dated: July 09, 2021

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Kevin O’Donnell
Henry & O’Donnell P.C.
300 N. Washington St, Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
kmo@henrylaw.com

Paul J. Andre
Lisa Kobialka
James Hannah
Kris Kastens
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com
hlee@kramerlevin.com

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, INC.

DEMAND FOR JURY TRIAL

In accordance with Rule 38 of the Federal Rules of Civil Procedure, Plaintiff respectfully demands a jury trial of all issues triable to a jury in this action.

Respectfully submitted,

Dated: July 09, 2021

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Kevin O'Donnell
Henry & O'Donnell P.C.
300 N. Washington St, Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
kmo@henrylaw.com

Paul J. Andre
Lisa Kobialka
James Hannah
Kris Kastens
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com
hlee@kramerlevin.com

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, INC.